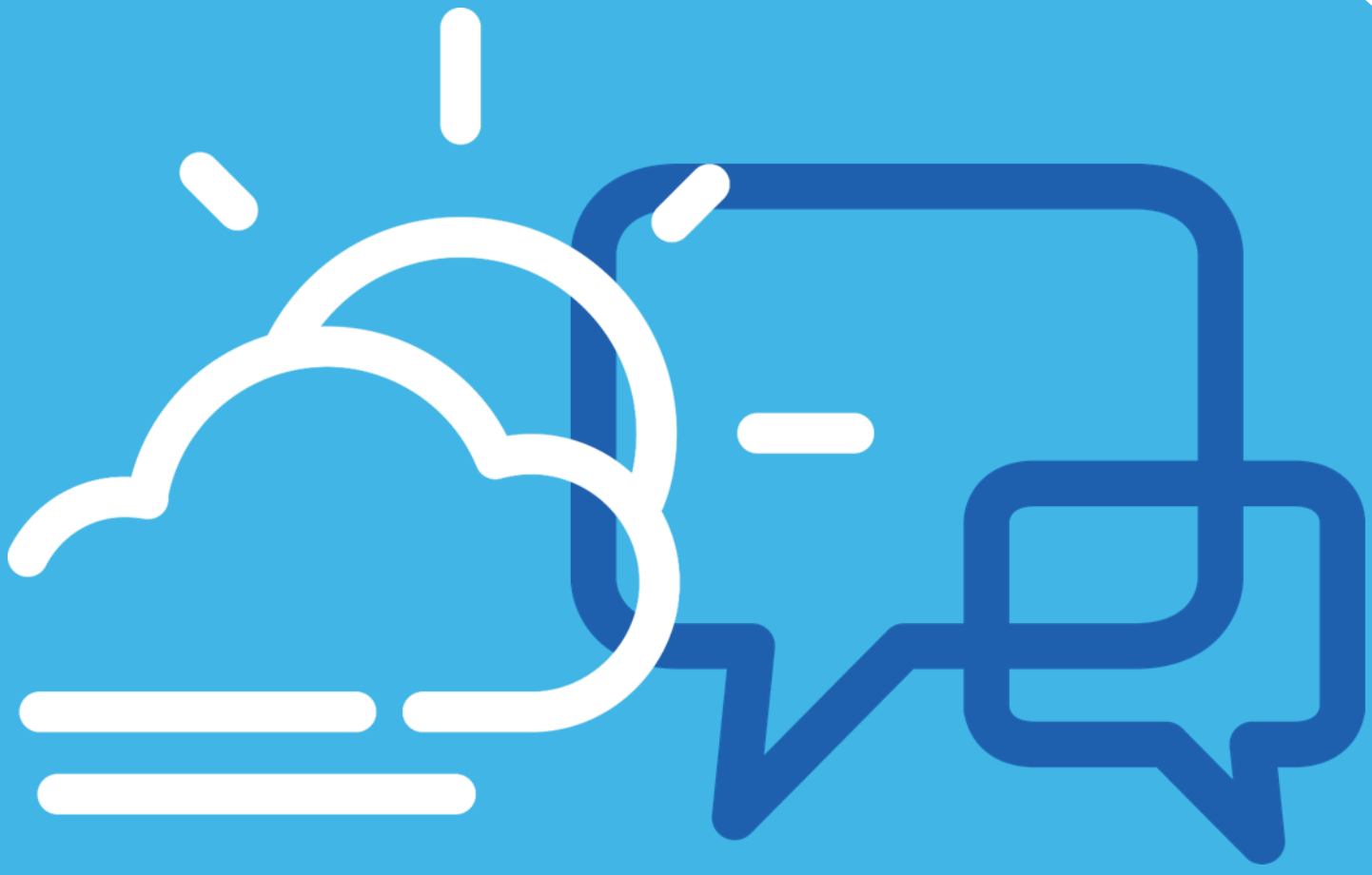
NHS
Greater Manchester Mental Health
NHS Foundation Trust

Clinical System Access Policy

Greater Manchester Mental Health NHS Foundation Trust



Improving Lives

Document Name:	**Clinical System Access Policy**
Executive Summary:	The policy aims to prevent unauthorised access to the electronic health records of Greater Manchester Mental Health NHS Foundation Trust.
Executive Lead:	Director of Finance, Capital and IM&T
Document Author:	Sarah McDonald (Head of IM&T Service Delivery)
Document Purpose:	Policy
Target Audience:	All staff legitimately able to access the Clinical System. Including GMMH employees, Bank Staff, Agency Staff and Third Parties.
Additional Circulation List:	All employees via Trust intranet
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 Information Governance Policy
Superseded Docs:	Former GMW Pseudonymisation Policy
Date of Equality Impact Assessment:	Pending
Board Objective Reference:	3 – To engage in effective partnership working 6 – To achieve sustainable financial strength and be well governed
CQC Regulation Reference:	Regulation 17: Good Governance Quality & Risk Profile
Risk Register Reference:	N/A
Contact Details for further information	Sarah McDonald (Head of IM&T Service Delivery) Email: sarah.mcdonald@gmmh.nhs.uk Tel: 0161 358 1751
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

This policy addresses access to the Clinical Systems, operated by Greater Manchester Mental Health NHS Foundation Trust. These systems are the Trust's electronic patient records and are used by all of the clinical services across the organisation. The Data Protection Act 2018 and General Data Protection Regulation (GDPR) require the Trust to implement technical and organisational measures to protect all personal data and information held by the system.

1.1. Purpose

The purpose of this Policy is to:

- ensure that users understand their obligations in relation to accessing the clinical information system;
- prevent unauthorised access to the Trust's electronic health records by implementing a robust registration and de-registration process for access;
- protect the confidentiality of the Trust's electronic health records by ensuring that access rights to patients' electronic records adhere to the principles of the Caldicott recommendations (HSC 1999/012), the Data Protection Act 2018 and the General Data Protection Regulation;
- ensure the security of the Trust's electronic health record meets the national standards stipulated in the Data Security and Protection Toolkit.

Service Users of the Trust expect that information in their clinical record will be treated as confidential. The Trust expects of all employees to recognise and act upon their responsibility to maintain patient confidentiality. The duty of confidentiality is confirmed in professional guidelines and contracts of employment.

Trust standards and expectations relating to information security and confidentiality are detailed in the Trust's Confidentiality Policy. Any breach of confidentiality with regard to the disclosure of, or inappropriate access to, patients' personal information held by the Trust is a disciplinary offence, and may result in dismissal and/or prosecution.

'Legitimate access' to a patient records is classed as 'A clinical reason to access the record'. It is not acceptable to simply search the Trusts systems. Should a staff member know a person open to services personally they should declare this to their line manager.

1.2. Scope

This policy is relevant to all trust employees. It is intended to be read in conjunction with the Trust's data security and protection policies and information management and technology polices. Taken together these policies provide a detailed overview of the Trust's approach to the management and use of information.

2. Definitions

- BI - Business Intelligence
- Clinical System - Clinical System such as PARIS
- CSO – Clinical Safety Officer
- Deputy SIRO – Deputy System Information Risk Owner
- DOP – Data Protection Officer
- HSC – Health Service Circular
- IAO – Information Asset Owner
- ID – Identification
- IEC - International Electro-technical Commission
- IG – Information Governance
- IGSG – Information Governance Steering Group
- IM&T - Information Management and Technology
- IPFM – Inpatient Flow Management
- IQA – Information Quality Assurance
- ISA - Information Sharing Agreement
- ISO – International Organisation for Standardisation
- RAG – Restricted Access Groups
- SCO – Clinical Safety Officer
- SIRO – System Information Risk Owner
- SSO – Single Sign On

3. Duties

3.1. Board/Lead Committee

The Information Governance Steering Group is responsible for the maintenance, updating and ratification of this policy, ensuring at all times that information is both up to date and relevant.

3.2. Senior Information Risk Owner

The Senior Information Risk Owner, (Director of Finance and IM&T), acts as an advocate for information risk on the Board and in internal discussions will provide written advice to the Chief Executive on the content of the Annual Statement of Internal control in regards to information risks.

The SIRO/Deputy SIRO will be responsible for accessing and reviewing all requests for pseudonymised records and restricted records.

3.3. Information Asset Owner

The Information Asset Owner (IAO) is the individual who has been assigned responsibility for the management of the Trust clinical information system Each critical asset used across the trust has an IAO assigned. Details of the owners and systems can be found in the key information asset register.

The IAO suggests objectives and priorities for the system, allocates resources,

commission system developments, design recording practices and oversee the delivery of training programs to users. This ensures the integrity and quality of the system, the management and resolution of any system issues and that the system is compliant with national standards.

3.4. Data Protection Officer

The GDPR introduces a legal duty to appoint a Data Protection Officer (DPO) for all public authorities and on organisations that carry out certain types of processing activities.

DPOs assist to 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 data subjects and the supervisory authority (ICO). The DPO must be independent, an expert in data protection, adequately resourced, and report to the highest management level.

The Trust's DPO will help demonstrate compliance and is part of the enhanced focus on accountability within the Trust.

3.5. Caldicott Guardian/Senior Medical Officer/Clinical Safety Officer

The Caldicott Guardian is a senior health professional nominated by the Trust to be responsible for safeguarding the confidentiality of patient information pursuant to recommendation 3 of the Caldicott Report 1997. The NHS IM&T Security Manual (Section 18.4) also requires each organisation to designate a senior medical officer to oversee all procedures affecting access to person-identifiable health data. In the Greater Manchester Mental Health NHS Foundation Trust these roles have been combined and are assigned to the Trust's Medical Director. The Caldicott Guardian is assisted in these roles by the Clinical Safety Officer (CSO) and the Information Governance Manager.

Clinical decisions are to be made by the Medical Director or in the absence of the Medical Director, the Deputy Medical Director. Advice and support should be sought as required from the Clinical Safety Officer and the Information Governance Team.

3.6. Information Governance Team

The IG Team must be consulted with about any issues relating to the governance of the clinical system and person-based/ person-identifiable information and its usage prior to implementation or changes being made.

The IG Team will assist Information Asset Owners, on request, in the implementation and monitoring of this Policy via the Information Governance Steering Group (IGSG).

The IG Team will ensure training is available via the learning hub to staff across the trust around the principles and good practice of all aspects of person identifiable information, the Caldicott recommendations, Data Protection and GDPR legislation.

3.7. Systems Team

The Systems Team are responsible for the management, configuration, administration and operational support of the clinical information system. The systems team are also responsible for ensuring the security configuration of the system adheres to the requirements of this Policy.

The systems team are also responsible for system development, upgrades, testing and ensuring that the system meets with national and local requirements.

3.8. IM&T Training Team

The IM&T Training Team will ensure that users of the system are provided with training as per Appendix E, so that staff can carry out their duties within the clinical information system, in a clinically safe manner. The GMMH Learning Hub will keep a central record of the training users have received. The Learning Hub also holds e-learning materials for the clinical information system.

3.9. IM&T Operations Team

The IM&T Operations Team are responsible for the creation and management of user accounts. The IM&T Operations Team are also responsible for the administration and control of the Authorised Signatories register.

3.10. Service Managers

Service Managers are responsible for ensuring that their staff adhere to the requirements of this policy and that any issues that arise from the implementation of the policy, or concerns about contraventions of the policy, are acted upon immediately.

3.11. Authorised Signatures

Authorised Signatures are key individuals who are responsible for determining if users should be granted access to the clinical system.

The IM&T Operations team will maintain the master list of authorised signatures. It is the responsibility of services to inform the IM&T operations team if the details within their area change.

3.12. System Users

To ensure that users are using the system in a clinically safe and legal manner and that they understand their responsibility in the protection of personal data that they are given access to, it is the principle that all GMMH staff are required to complete a training course along with a **competency based assessment.**

Exceptions to this rule would be medical staff who require access at short notice to be able to provide clinical care. These may be given access to the system on a temporary basis, e.g. out of hours, and directed towards the online training materials

and be given access the system.

Out of hours, the Trust on call staff member will be contacted by the on site manager, bronze on-call; for permission to create a new account. This manager must provide all user details in an email to IM&T and cc'd to Trust on call to evidence that a conversation has taken place to authorise, before any new accounts can be created. It is the requesting manager's responsibility to inform IM&T when the access is no longer required by the short term user by logging a request with Support Central to revoke the access.

Any short term account access circumstances are followed by the user needing to attend a course within 30 days. If adherence with the exception criteria outlined below is not followed, access will be removed.

Exceptions must be kept to a minimum and only with strict adherence to the following criteria:

1. The operational manager responsible for the individual is fully aware and agrees to be responsible for any actions undertaken by the individual within the Clinical System.
2. The individual does attend a training course within 30 days.
3. The individual completes the online competency based assessment after attending the training course.
4. The individual is fully compliant with their IG training within 30 days.
5. Users have legal, professional and ethical obligations to safeguard the confidentiality of patients' records and to protect this information from unauthorised disclosure or misuse. Users must not share or write down their password. Users also have an individual responsibility to ensure that the requirements of this Policy are observed and to raise any concerns that they may have regarding inappropriate or unprofessional use of the information system.

4. System Access

4.1. System Users

This policy applies to all of the Trust's staff and staff employed by partner organisations including non-health care providers who, during the course of their duties, will require access to the information held on the clinical information system. Please note volunteers do not have access to the Trust's clinical information system. Member of the clergy will not be granted access to the clinical system; should the need and/or request to share information arise this can be done with the client's consent using other communication methods such as providing a copy of the latest risk assessment or via a conversation with the clients clinical team.

4.2. System User Registration

New system users, including those requiring read only access, will be required to complete an electronic access request form available from the Service Desk portal,

which will need to have an authorised countersignatory (Approver) selected. Users must indicate that they have read and understood this policy and attach their certificate of IG compliance to the request form. Amendments to existing accounts will need to be completed via the same method as new system users.

Each request for access to the system will be considered individually to ensure that the request is clinically appropriate and that the relevant access rights are granted.

Where the applicant for an account is a Researcher, the request for the read only account is made by the Research & Innovation Department, with the relevant R&I counter signatory (Approver) selected. This is to ensure the researcher is working on a research project where access to medical records with patient consent has been approved by an Ethics Committee, or, where appropriate approval under Section 251 (access to medical records without patient consent) has been given by the Health Research Authority (HRA).

4.3. Access for Staff Employed by Third Parties

There may be occasions when, in order to support seamless pathways of care for service users, external agencies or partner organisations request that their staff are granted access to the system.

An external agency may include (but not limited to):

- another NHS Trust;
- local authority;
- voluntary sector provider;
- private sector provider.

An Information Sharing Agreement (ISA) or a Data Protection Impact Assessment will need to be completed and agreed by both the requester and the Trust and approved before any system access is granted. The process for this is outlined in the Information Asset Management Policy and Information Sharing Policy.

All third party personnel requiring access to the clinical system will need to complete the required system training Including completed Information Governance training. Third party personnel that require both read and write access will need to undertake the appropriate GMMH training course for their role.

All requests for access to the clinical system by external agencies will be reviewed by the IG Team. A regular update is provided to the IGSG on information sharing agreement status.

4.4. Inpatient Patient Flow Management System Access

The Inpatient Flow Management (IPFM) system is an integral part of the clinical information system.

Each IPFM user has a username and password created, which they log in with for the

first time only. Following initial log in, users no longer have to remember their passwords as it remembered by the Trust Single sign on application and is part of the single sign on process (described below in 4.7 Password Management).

The user name and password allow users to view the system but does not allow them to record any information. To allow users to record information, the users are issued a 6 digit numeric pin code, which they need to enter every time they record an entry into the system.

The amount of access given to users is role based. For example System Administrators would be given full access, whilst ward staff would be restricted to certain activities as required to undertake essential duties.

New users are given access to the system on completion of the user access form submitted via IM&T Support Central.

4.5. Additional Access Requirements

GMMH may need to provide access to clinical information to a number of groups including and not limited to: Legal Advisors, Auditors, Commissioners, Police Officers, Independent Medical Staff, Independent Mental Health Advocates and Mental Health Act Commissioners.

Dependant on the request, access may be granted via the subject access request process or via the supervised system access process, see Appendix D.

Supervised access to the clinical system will be supported by a nominated member of GMMH staff to be able to access the relevant information in a timely manner.

The IG team must be notified of each occurrence of supervised access in advance via the supervised system access proforma. A register of all supervised access will be maintained and the IGSG will be updated on a regular basis.

4.6. Notification of De-activation of Accounts

Line Managers are responsible for requesting the deactivation of Clinical System accounts when members of their team leave the Trust.

The manager will be ultimately responsible for all transactions that take place on accounts that should be closed and are still active as a result of non-notification on behalf of the manager. Requests for the deactivation of accounts must be made by written request via IM&T Support Central.

4.7. Password Management

Clinical System passwords are managed by the user's network login details and a utility known as Single Sign On (SSO).

The first time a user logs in to the clinical system with their issued username and password, SSO learns these details and the user never has to enter them again.

Network passwords are configured to be changed every 30 days and since SSO manages the user login process, users are never prompted to change their clinical system or IPFM password.

Clinical system users will be solely responsible for all system transactions conducted under their network account details.

Passwords will be never be issued to users over the telephone. The IM&T Operations Team will send an email directly to the user's registered email address, or in the case of an out of hours request, the email will be sent to Site Manager/ On Call. The IM&T Operations Team will issue a temporary single use password for the clinical system and IPFM which SSO will automatically change on first login.

4.8. Review of User Accounts

The IM&T Operations Team will conduct a monthly review of the use of all active clinical system user accounts. Accounts that have not had a successful log in during the previous 90 days will be de-activated immediately. A request for re-activation of the account must be made via IM&T Support Central and approved by an 'Authorised Signatory' as per section 4.2 - System User Registration.

4.9. System Security

4.9.1 Safeguarding Service User Information

In order to ensure that Service User information is accessed, transferred, used and stored in line with the Information Governance principles outlined in this document the Trust has introduced a number of safeguards.
The safeguards in place to ensure safe usage include but are not limited to the following:

- Access Monitoring
- Restricting Access
- Pseudonymisation
- Physical Access Controls

4.9.2 Access Monitoring

In the clinical system, all users need to belong to a clinical team (or multiple teams) which determine a user's system access. As a user, you have the ability to view information across the clinical record but only add/amend when you are part of the service user's clinical team.

The IG Team is responsible for ensuring that there is a system in place to monitor inappropriate access, in order to achieve this an access monitoring audit tool has been developed.

The audit tool will run routine audits against user access to alert the Trust to possible breaches of confidentiality or unauthorised or inappropriate access made by a user. Any instances of inappropriate access will be pro-actively investigated and could result in disciplinary action being undertaken.

Managers may request information from the IG Team if they suspect inappropriate access and have concerns around any user misusing the system. Information may be requested via completion of the Clinical System audit form, see **Appendix A.**

The term 'inappropriate access' means accessing a service user clinical record when you do not have a legitimate reason to do so. Inappropriately accessing information in this way could result in disciplinary action being instigated, see **Appendix B.**

Legitimate access is defined by having a business requirement in the line of your duties to access that record. For clinical staff this would mean being involved in the clinical care.

All staff have been advised that the inappropriate access of Service User information is in direct violation of the Data Protection Act 2018 and General Data Protection Regulation and as a result would be reportable to the Information Commissioner's Office for further investigation and possible criminal conviction.

4.9.3 Pseudonymisation

Pseudonymisation is the process by which personal identifiable information is removed with the sole purpose of enhancing individual security. This should be applied only in cases where the information is considered to be of significant importance and sensitivity that if used in its original form could lead to a significant incident. In the clinical information system, the NHS number will remain present as the identifier for the service user (with other personal details being removed name etc.)

Pseudonymisation should be applied in the clinical system in exceptional circumstances only, as this activity can affect clinical care decision making if clinicians are unaware of clinical events and updates. The following general criteria applies, but is not exhaustive:

- High Profile Patient i.e. potential for general and media interest
- Patient is a member of Trust staff
- Concern at having their details accessible
- Undue stress at having their details accessible
- Refusal to continue treatment if details remain accessible

As an alternative to Pseudonymisation, Special Indicator monitoring must be considered with the patient. This is outlined, and can be requested, in the form at **Appendix B**.

The process for pseudonymisation requires completion of a Patient Record Special Indicator & Pseudonymisation Request Form **Appendix B** by the Clinician in conjunction with the patient. The form is then forwarded to the IG Team who register the request, before sending this to the SIRO or Deputy SIRO for approval. Once approved, the IG Team will Pseudonymise the record.

The service user along with their named clinician will be required to provide rationale for having their record pseudonymised. If the request is approved, the SIRO will inform the Information Governance Department of the details of the pseudonymisation, including the activation date. The IG team will feedback the outcome to the named clinician.

Pseudonymisation will be applied for a temporary period if appropriate, rather than a long term application. Any decision appeals will be forwarded to the Caldicott Guardian.

It is a requirement that the need for the patient record to remain Pseudonymised is reviewed on a regular basis, and at the point of discharge or when the circumstances provided as rationale for pseudonymisation change.

4.9.4 Restricted Access

Documents are able to be stored outside the clinical information system if it is deemed appropriate that they are not available to all as part of the clinical record. Documents are stored in secure electronic folders with a group membership for access. Any member of this group is able to view the relevant restricted service user information.

Staff should be aware that the use of restriction on clinical information increases the risk of Serious Untoward Incidents.

All requests for the use of restricted information will be requested by the Information Asset Owner via an online registration form on IM&T Support Central. All requests will be sent and reviewed by the IG team, who will then forward the request on to the SIRO (Director of Finance and IM&T) for final approval. In the SIRO's absence all requests will be approved by the Deputy SIRO (Head of IM&T Service Delivery). If the restriction is approved, the relevant document needs to be uploaded onto the Share point library area, see **Appendix C.**

An alert will be entered on the clinical information system to record that restricted records exist for this service user as these need to be considered for subject access requests etc.

It is the responsibility of service managers to notify IM&T Support Central if any staff members included within that restricted access group leave, so that the group membership maybe updated.

4.9.5 Physical Access Controls

All users of the clinical information system must take appropriate precautions to ensure that unauthorised personnel cannot gain access to the system. Computers should be positioned where they are only accessible to authorised users. Where this is not viable, display screens and printers must be positioned to avoid accidental disclosure. Equipment must not be left unattended unless it has been locked or switched off.

Users should always log out of the clinical information system as soon as it is no longer required, as this will reduce the risk of inappropriate disclosure.
Offices with computers should always be locked whenever they are unoccupied.

Users of the clinical system must not store patient-related information on their hard drives. All non- restricted clinical information must be stored within the clinical system.

4.9.6 Breaches of the Clinical Information System Security

A breach of clinical information system security is described as but is not limited to:

- Actual or potential unauthorised release of information from the system.
- Use of another user's network login and password.
- Deliberately accessing information not relevant to the user's role in:
    - the assessment, planning and delivery of care to the patient.
    - the maintenance of the system or data.

Staff employed by the Trust
Any breach, or suspected breach, of Clinical System security must be reported directly to the IG Team and recorded on the incident management system.
The IG Team will subsequently report any concerns of actual or suspected breach to the SIRO. Any Information Governance incidents recorded as a level 4 or 5 on the incident management system will be reported to the Information Commissioner's Office by the IG team.

A breach of Clinical System security is considered an act of gross misconduct and could be considered as a criminal offence. Any breach or suspected breach from any member of staff as stated in the policies target audience will result in an internal investigation by GMMH, and may render the user liable to disciplinary action or dismissal irrespective of their place of work.

Staff employed by third party organisations
If a third party organisation wants to view a record of a service user but by doing so will fall outside the original remit agreed within the Information Sharing Agreement, the audit tool will alert this occurrence and this will be highlighted to the Authorised Signatory who will raise this with the third party lead.

Any breach, or suspected breach, of security by a non-Trust employee must be reported directly to the Trust's IG Team.

Should there be instances where a third party accesses a record inappropriately, the outcome of the discussion between the authorised signatory and the third party lead will be sent to the IG team and forwarded to the SIRO/Deputy SIRO for review and appropriate action to be taken.

All investigations around breaches of security must be detailed within any contract or Information Sharing Agreement.

Staff employed by an agency

Any breach, or suspected breach, of security by a non-Trust employee must be reported directly to the Trust's IG Team. Additionally, the breach should be reported to the locum agency's senior manager for action in line with that organisation's standard procedures for dealing with breaches of confidentiality.

Locums employed directly by the Trust

Any breach, or suspected breach, of security must be reported directly to the IG Team.

5. Training Requirements

Awareness training for this policy will be delivered as a component of IM&T Training delivery.

Information Governance Training must be undertaken by all users of IM&T systems on an annual basis.

6. Monitoring

Minimum Requirement	Frequency	Process for monitoring	Evidence	Responsible Individual(s)	Response Committee(s)
Proactive access audits	As and when required	Audit Tool	Reporting to SIRO and reporting incidents	All staff	IGSG

7. Resource/Implementation Issues

N/A

8. Risk Issues

There are risks attached which include but are not limited to the following:

- Staff sharing ID information.
- Staff being granted access to the clinical system contrary to the 'no training no access' policy.
- Staff and third parties accessing inappropriate information without legitimate cause.
- Individuals being able to view information from other teams.

9. Requirements, Supporting Documents and References

9.1. Requirements

Board Objective Reference:	3 – To engage in effective partnership working 6 – To achieve sustainable financial strength and be well governed

CQC Regulation Reference:	Regulation 17: Good Governance Quality & Risk Profile
Other obligations:	Legislation including • Data Protection Act 2018 • The General Data Protection Regulation • Caldicott Recommendations (HSC 1999/012) • ISO/IEC 17799:2005 - Code of Practice for Information Security Management

9.2. Supporting Documents

- Information Security Management - NHS Code of Practice
- Data Security and Protection Toolkit - Good Practice Guidelines
- Access to Health Records Procedure
- Confidentiality Policy
- Information Security Policy
- Records Management Policy
- Standard and Structure of Clinical Health Records
- On-call procedure
- Incident Accident and Near Miss Policy

9.3. References

- Data Protection Act 2018
- The General Data Protection Regulation
- Caldicott Recommendations (HSC 1999/012)
- ISO/IEC 17799:2005 - Code of Practice for Information Security Management

10. Subject Expert and Feedback

For advice on this policy please contact the IG team via IM&T Support Central.

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.

12. Appendices

See following pages.

Appendix A – Clinical System audit request form

CONFIDENTIAL

Request for audit form

Please complete all sections of this form.

The request must be approved by the Information Asset Owner.
Please complete sections 1 – 5 and email to informationgovernance@gmmh.nhs.uk

1. **Person the audit is to be carried out on:**

Name:	
Job title:	
Base:	
IP address:	

2. **System to be audited:**

Email:	
Internet:	
PARIS:	
Amigos:	

3. **Background to/reason for request:**

4. **Specifics of audit requested: e.g. times, dates, PARIS ID's.**

5. **Person requesting audit**:

Name:	
Job title:	
Designation to above person:	
Contact details:	

Information Asset Owner Authorisation: IAO is usually Head of Services or Associate Director	An authorisation email can be sent from the authorising IAO to informationgovernance@gmmh.nhs.uk

Please note
IM & T staff will treat this as a matter of strict confidence. In some cases, they will need to remove the PC concerned for investigations. From the time your request is logged, IM&T staff will keep written notes of action taken, which will form an audit trail.

IT staff can provide advice/evidence from a technical perspective only.

If you have questions about how the evidence should be treated in regard to a disciplinary policy/investigation, please contact the HR department.

To be completed by the Information Governance Team

6. **Is the request for audit approved?**

Date request received:	
Audit request reference:	
Is audit approved?	Yes No – Reason?

7. **Feedback from audit findings:**

Appendix B – Patient Record Special Indicator & Pseudonymisation Request Form

PARIS [and PCMIS] Patient Record Special Indicator & Pseudonymisation Request Form

Please return completed form to: informationgovernance@gmmh.nhs.uk

Important Information

Consideration should be given to other information safeguards available prior to completion of this form.

Pseudonymisation should be applied in exceptional circumstances only as it removes all person identifiable information from the patient's record meaning that in an emergency situation, a name search of the clinical system will not return the patient's information. Therefore, without the provision of an NHS Number, vital patient data relative to their care cannot be accessed.

Patients must therefore be asked to consider the alternative measure of having a Special Indicator applied to their record which will result in daily monitoring of access by the Fair Warning alert system. There are a number of indicators which can be selected from below.

Fair Warning will raise an alert when these records are accessed and these are subsequently investigated. Where a record is found to have been accessed for any reason without authorisation, the Trust will take immediate, formal action against any personnel involved.

Additional recommended reading: Section 4.9.2 and 4.9.3 GMMH Clinical System Access Policy.

Patient PARIS ID	
Patient PCMIS ID	
NHS No.	
Date of Request	
Clinician	
Clinician Email	

Please select required data safeguard:

☐ FairWarning Special Indicator Request

Please select the relevant Special Indicator for the patient from the list below:

☐ High Profile Patient i.e. potential for general and media interest (HP)

☐ Patient is a member of Trust staff (SP)

☐ Close Monitor Flagged Patient (CM)

Or

☐ Pseudonymisation Request

Continued overleaf

Please ensure the following information is fully completed by all relevant persons.

In so doing, you are confirming that the patient has the capacity to make this decision and that they are aware of the potential risks associated with having their patient record pseudonymised.

Please confirm as above ☐ *If this box is not checked, Pseudonymisation will not be actioned.*

Patient Rationale

On what grounds is the patient requesting Pseudonymisation?

Select all that apply:

☐ High Profile Patient i.e. potential for general and media interest

☐ Patient is a member of Trust staff

☐ Concern at having their details accessible

☐ Undue stress at having their details accessible

☐ Refusal to continue treatment if details remain accessible

☐ Other, please state:

Clinician Rationale

Please state your reasons for supporting this application for Pseudonymisation:

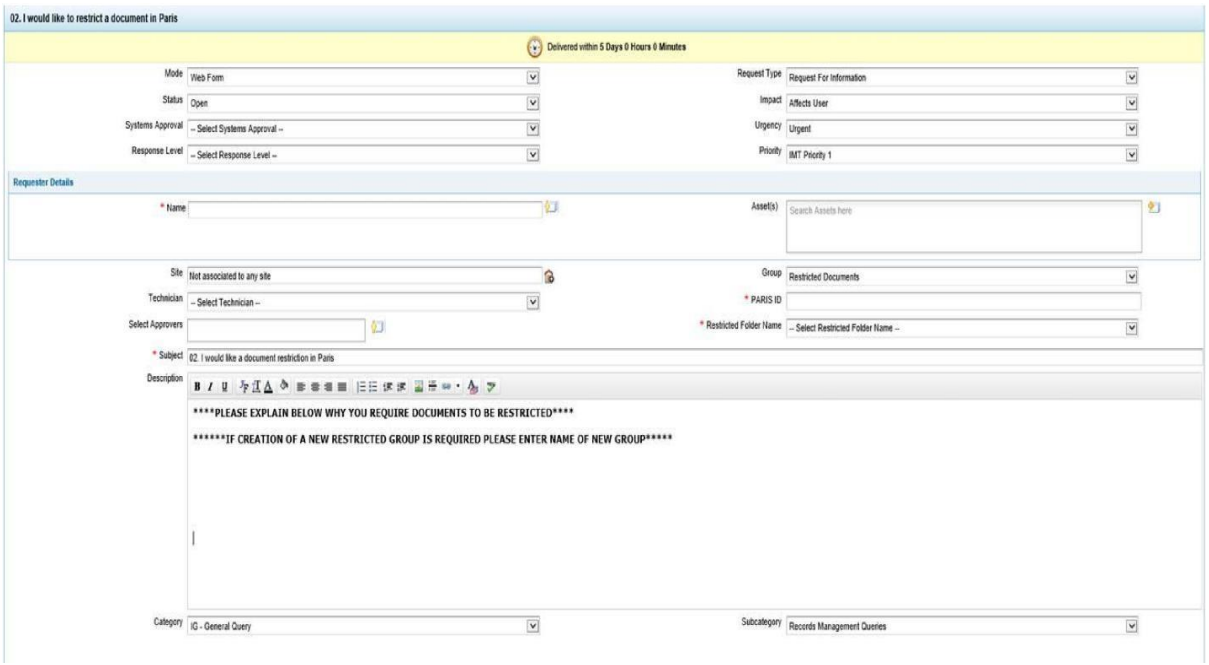
Date for de-Pseudonymisation, if appropriate: / /

SIRO/Deputy SIRO Rationale

I have ☐ Approved ☐ Not Approved

this request for Pseudonymisation on the following grounds:

Appendix C – Restricted Document Request



Appendix D – External Provider Request Form

External Provider Request Form in Clinical System

Requests for External providers to have access to Clinical System must be made to the Trust's Information Governance Department. If the request is approved, the IM&T Systems Team will create the Clinical System provider account.

Please note: External Providers must be supervised by a clinician/manager whilst they are accessing Clinical System.

Name of person requesting access	
Occupation	
Work Base Address (inc Post Code*)	
Work Base Telephone Number	

Clinical System Client ID:	

Area of speciality This indicates which client group the new provider works with. Place tick in appropriate box.	**Adult**	
	Child & Adolescent	
	Forensic Psychiatry	
	Learning Disability	
	Old Age Psychiatry	
	Other	

Rationale

Please can you briefly explain why you need to have access to this client's the clinical System record?

SIRO/Deputy SIRO Rationale

Please ensure that all requests for access are made with at least 5 working days' notice so this has time to go through the correct approval trail. Failure to adhere to this will result in access being delayed.

Appendix E – Clinical System Training Sessions

Clinical System Training Sessions

- **Community CPA & Non CPA Admin Combined (1 Day)**
  This one day course is for administrative staff from all community based services.

- **Community CPA & Non-CPA Clinician Combined (1 Day)**
  This one day course is for clinical staff in 'qualified roles' from all community based services (except medics) e.g. CPNs, Social Workers, Keyworkers and any other staff that use the staff Diary to plan their week.

- **Inpatient Admin (1 Day)**
  This one day course is for administrative staff from all inpatient ward or unit based services.

- **Inpatient Clinician (1 Day)**
  This one day course is for clinical staff in 'qualified roles' from all inpatient ward or unit based services (except medics) e.g. Staff Nurses, Team Leaders and Ward Managers.

  We recommend any staff that do not cover inpatient admissions, IPFM, leave and ward discharges, attend instead, the Community CPA & Non-CPA Clinician Combined (1 Day) course, as this will include Caseload Management and Staff Diary. This is likely to include staff in roles such as Physiotherapists, Dietitians and Occupational Therapists.

- **Medics (1 Day)**
  This one day course is for Medic staff based in both community and inpatient services from rotation level to Consultant.

- **Unqualified (½ Day)**
  This half day course is for clinical staff in 'unqualified roles' from all services, both community and inpatient, e.g. Students, Trainees, Assistants, STRs and Support Workers.

- **Pharmacy (½ Day)**
  This half day course is for Pharmacy staff.