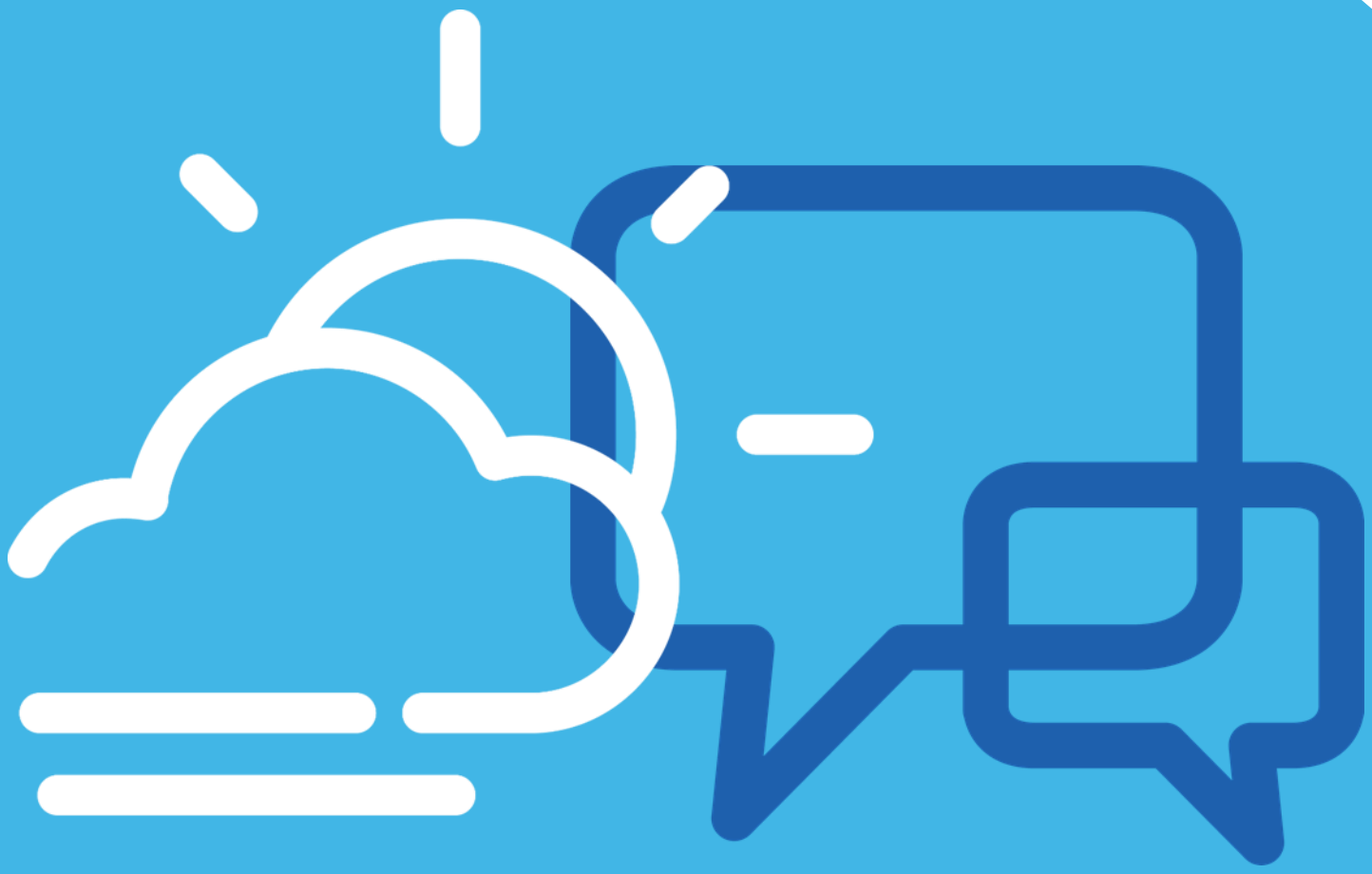
NHS
Greater Manchester Mental Health
NHS Foundation Trust

# Records Management Policy

Greater Manchester Mental Health NHS Foundation Trust



Improving Lives

| | |
|---|---|
| **Document Name:** | **Records Management Policy** |
| **Executive Summary:** | This policy has been developed to ensure that there is a systematic and planned approach to the management of all records within Greater Manchester Mental Health NHS Foundation Trust (GMMH), from their creation to their ultimate disposal.<br><br>The ultimate ambition of the Trust is that all areas are working electronically and as paper free as possible. However, it is recognised that at this point in time, there are both electronic and paper systems in use. The expectation is that where electronic systems exist they will be used. Paper systems used are by exception and agreement only. |
| **Executive Lead:** | Director of Finance and IM&T |
| **Document Author:** | Information Quality Assurance (IQA), IM&T |
| **Document Purpose:** | Policy |
| **Target Audience:** | All Employees |
| **Additional Circulation List:** | All Employees via the Trust Intranet |
| **Date Ratified:** | 13/02/18 |
| **Ratified by:** | Information Governance Steering Group |
| **Consultation:** | Via SharePoint Consultation System |
| **Cross Reference:** | N/A |
| **Superseded Docs:** | GMW – Records Management Policy<br>MMHSC – Service User Care Records Management Policy Corporate Records Management Policy |
| **Date of Equality Impact Assessment:** | 13/11/17 |
| **Board Objective Reference:** | 6 - Achieve sustainability financial strength and be well governed |
| **CQC Regulation Reference:** | Regulation 17: Good Governance |
| **Risk Register Reference:** | N/A |
| **Contact Details for further information** | Information Quality Assurance via:<br>IQA@gmmh.nhs.uk<br>0161 271 0040 |
| **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

'Records Management' is the process by which an organisation manages all the aspects of records, whether internally or externally generated, and in any format or media type; from their creation, all the way through to their lifecycle to their eventual disposal.

All NHS records are Public Records under the Public Records Acts and must be kept in accordance with the following statutory, governmental and NHS requirements:

- Public Records Acts (1958) and (1967)
- Data Protection Act (1998)
- Freedom of Information Act (2000)
- The Common Law Duty of Confidentiality
- Lord Chancellor's Code of Practice on the management of records under Section 46 and the Freedom of Information Act (2000).
- Records Management Code of Practice for Health and Social Care 2016 (RMCoP)
- Independent Inquiry into Child Sexual Abuse (IICSA).

The ultimate ambition of the Trust is that all areas are working electronically and as paper free as possible. However, it is recognised that, at this point in time, there are both electronic and paper systems in use. The expectation is that where electronic systems exist they will be used and that paper systems used are by exception and agreement only.

This document sets out a framework for consistent and effective records management that is based on established standards which are aligned with other information governance work areas such as confidentiality and information security. It will enable staff with responsibilities for managing Trust records to develop operational procedures that will ensure records are managed and controlled effectively, and at best value, commensurate with legal, operational and information needs

## 1.1. Purpose

Specific aims of the Trust's approach to Records Management are to ensure that:

- Adequate records are maintained to fully and transparently account for all actions and decisions.
- Records are complete and accurate, and the information they contain is reliable.
- Records can be used and maintained through time – the qualities of availability, accessibility, interpretation and trustworthiness can be maintained for as long as the record is needed, perhaps permanently, despite changes of format.
- Records can be easily retrieved by those with a legitimate right of access, when needed, for as long as the records are held by the Trust, and can be located and displayed in a way consistent with their initial use. Where multiply

versions exist, the current version is identified.

- Records are secure - from unauthorised or inadvertent alteration or erasure, that access and disclosure are properly controlled and audit trails will track all use and changes. To ensure that records are held in a robust format which remains readable for as long as records are required.
- Records are retained and disposed of appropriately - using consistent and documented retention and disposal procedures, which include provision for appraisal and the permanent preservation of records with archival value.
- Staff are trained - so that all staff employed by or on contract to the Trust are made aware of their personal and organisational responsibilities for record-keeping and records management.

### 1.2. Scope

This policy applies to all Trust records, regardless of the media on which they are created or held, or the functional area they are created or held by.

Records are defined by the ISO standard, ISO 15489-1:2016 Information and documentation - Records management defines a record as 'information created, received, and maintained as evidence and information by an organisation or person, in pursuance of legal obligations or in the transaction of business'.

The Data Protection Act 1998 (DPA) S68(2) defines a health record which 'consists of information relating to the physical or mental health or condition of an individual, and has been made by or on behalf of a health professional in connection with the care of that individual'.

Examples of records that should be managed using this policy are:

- Paper records, including records held in offsite storage.
- Electronic records e.g. email, network, scanned, websites.
- Photographs, slides and other images.
- Microform e.g. microfiche, microfilm.
- Tapes held on CCTV and other visual recordings.
- Text messages and social media e.g. Facebook, twitter.
- Other electronic media, CD-ROM/DVDs, memory sticks, audio recordings.
- Clinical services e.g. health records.
- Corporate services e.g. customer care, complaints, investigations, claims, incidents, personnel, estates and finance.

## 2. Definitions

| | |
|---|---|
| Appraisal | The process of evaluating an organisation's activities to determine which records should be kept, and for how long, to meet the needs of the organisation, the requirements of Government accountability and the expectations of researchers and other users of the records. |

| | |
|---|---|
| Current records | Records necessary for conducting the current and ongoing business of an organisation. |
| Destruction | The process of eliminating or deleting records beyond any possible reconstruction. |
| File | An organised unit of documents grouped together either for current use by the creator or in the process of archival arrangement, because they relate to the same subject, activity or transaction. A file is usually the basic unit within a records series. |
| Information | Is a corporate asset. The Trust's records are important sources of administrative, evidential and historical information. They are vital to the Trust to support its current and future operations (including meeting the requirements of Freedom of Information legislation), for the purpose of accountability, and for an awareness and understanding of its history and procedures. |
| NHS records | All NHS records are public records under the terms of the Public Records Act 1958 sections 3(1)–(2). All records created and used by NHS employees are public records. |
| Permanent preservation | Records may not ordinarily be retained for more than 30 years. However, the Public Records Act provides for records which are still in current use to be legally retained.<br>Section 33 of the Data Protection Act permits personal data identified as being of historical or statistical research value to be kept indefinitely as archives |
| Records | In this policy, records are defined as 'recorded information, in any form, created or received and maintained by the Trust in the transaction of its business or conduct of affairs and kept as evidence of such activity'. |
| Records life cycle | A description of the life of a record from its creation/receipt through the period of its 'active' use, then into a period of 'inactive' retention (such as closed files which may still be referred to occasionally) and finally either confidential disposal or archival preservation. |
| Records management | A discipline which utilises an administrative system to direct and control the creation, version control, distribution, filing, retention, storage and disposal of records, in a way that is administratively and legally sound, whilst at the same time serving the operational needs of the Trust and preserving an appropriate historical record. The key components of records management are:<br>record creation;<br>record keeping;<br>record maintenance (including tracking of record movements);<br>access and disclosure;<br>closure and transfer;<br>appraisal;<br>archiving and<br>disposal. |
| Review | The examination of records to determine whether they should be destroyed, retained for a further period, transferred to an archival establishment, or presented to a third party (for example a University). |

| | |
|---|---|
| Tracking | Creating, capturing and maintaining information about the movement and use of records. (BS ISO 15489-1:2016(E)) |

# 3. Duties

## 3.1. Board/Lead Committee

The Information Governance Steering Group (IGSG) is responsible for providing scrutiny and review of this document prior to approval.

The IGSG will monitor and oversee the implementation of this policy.

## 3.2. Chief Executive

The Chief Executive is responsible for ensuring that GMMH implements a records management policy which is fit for purpose and complies with all relevant legislation. The Chief Executive delegates executive responsibility to the Director of IM&T.

## 3.3. Executive Directors

### 3.3.1 Director of IM&T and Finance

The Director of IM&T has lead responsibility for formulating the Trust approach to records management, incorporating policy and process development. To include approval, compliance with, monitoring and review of any documents produced.

In addition, the Director of IM&T is the Trust Senior Information Risk Owner and is therefore accountable for management of all Trust information assets, including managing information risks and incidents.

The Director of IM&T delegates policy and process development to the IQA Manager and operational responsibility to Information Asset Owners.

### 3.3.2 Director of Nursing and Governance

The Director of Nursing and Governance is the Caldicott Guardian. They have an advisory role which is concerned with the management and sharing of patient information

## 3.4. Managers

### 3.4.1 Information Quality Assurance (IQA) Manager

The IQA Manager is responsible for the overall development and maintenance of records management practices throughout the Trust. In particular the IQA Manager is responsible for drawing up guidance for good records management practice and promoting compliance with this policy. The IQA Manager will also monitor records management systems and practices across the Trust.

They will provide professional advice and support to all employees in relation records management.

### 3.4.2 Information Asset Owners (IAO)

Information Asset Owners are accountable for the information assets in their business area / service and as such are responsible for records management. They must ensure the requirements of this policy are applied / implemented and that all staff are adequately trained to apply the appropriate guidelines.

### 3.4.3 Information Asset Administrator (IAA)

Information Asset Administrators will support the Information Asset Owners on a day to day basis and will therefore support the implementation of this policy in their business area / service as delegated by the IAO

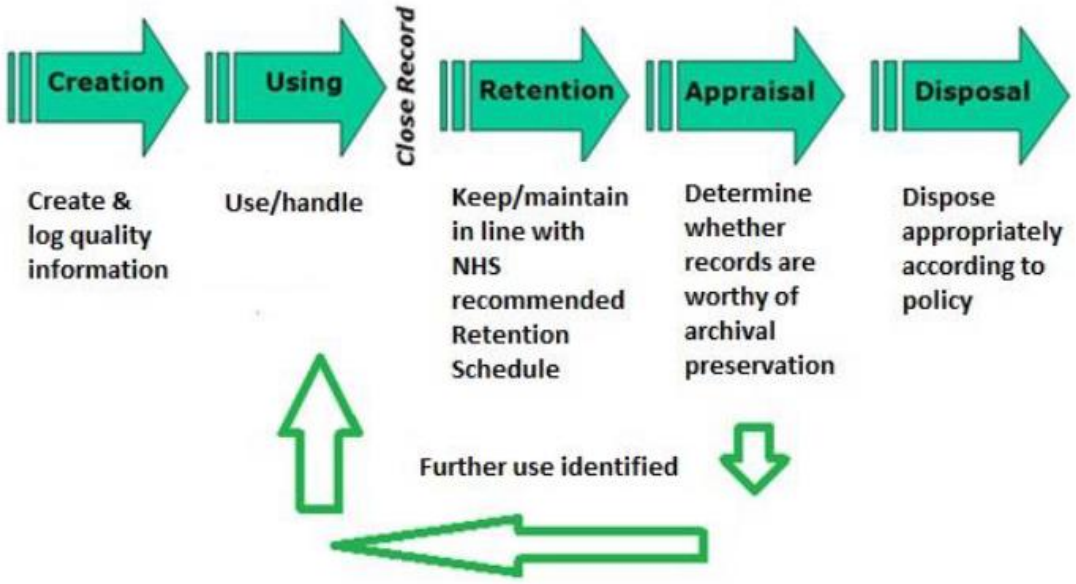
## 3.5. Employees

Under the Public Records Act 1958 employees are responsible for any records that they create or use in the course of their duties. Therefore, any records created or received by an employee of the NHS are public records and may be subject to both legal and professional obligations.

All employees must comply with this policy and all associated records management procedures.

# 4. Processes and Procedures

Figure 1 - The Records/Information Lifecycle



## 4.1. Record Creation

Record series will be declared via the Trust Information Asset Management process and will be recorded on asset registers under the responsibility of the Information Asset Owner, supported by Information Asset Assistants.

Each operational area of the Trust, including third party organisations that are providing services on the Trust's behalf, must have adequate systems in place for documenting their activities, (where appropriate), particularly where the activities/services are in relation to the provision of business activities or patient care.

Records should be complete and accurate enough to allow employees and their successors to:

- facilitate an audit or examination of the activity or functions performed;
- protect the legal rights or other rights of the Trust, its clients and any other person affected by its actions;
- provide authenticity of the records so that the evidence derived from the records is credible and authoritative.

When creating information in the first instance, the following should be adhered to, the information must be:

- available when needed - To enable a reconstruction of activities or events that have taken place;
- accessible to all members of staff who require access in order to enable them to carry out their day to day work;
- interpretable, clear and concise - The context of the information must be clear and be able to be interpreted appropriately, i.e. who created or added to the record and when this occurred;
- trusted, accurate and relevant - The authenticity must be demonstrable and the content relevant;
- secure - the information must be secure from unauthorised or inadvertent alteration, erasure while in use, storage or transfer or transportation both within and outside the Trust;
- access and disclosure - This must be properly controlled and audit trails used to track all use and changes. The information must be held in a robust format which remains readable for as long as the information is required or retained.

Records will be created and information captured in such a way that it is:

- legible;
- authored; signed with name and designation of the author printed below the signature, if the record is a written record. This should be completed after each entry;
- countersigned or approved where professional authority is required;
- recorded in black ink, if this is a written record;

- date and time stamped;
- contemporaneous;
- timely;
- version controlled;
- validated.

Records should be held in a relevant filing system as soon as possible after creation. For electronic records, this may be a secure shared network drive or other approved Trust software. Records should be filed in such a way that it is clear what the record contains and the organisational context in which it was created. Referencing, titling and indexing systems should be logical and easy to understand. The record should be easily retrievable and filed in such a way that the information can be promptly destroyed, in accordance with the retention schedules of the Records Management Code of Practice for Health & Social Care, when it is no longer needed.

Where records have a direct relationship with other collections of records in the Trust, this should be explicitly documented to enable a full record to be retrieved. This is particularly important where patient information is held separately from the main patient case file.

All records should be legible and accurate. Where personal data is concerned, it is a requirement of the Data Protection Act 1998 that personal data 'shall be accurate and where appropriate, up to date'.

In order to ensure that records are authentic and accurate, they should be created as soon as possible during or after the activity to which they relate. Records created long afterwards are more open to challenge in the event of a legal dispute.

Records will be created and used only for the purpose for which they are intended.

Records created by the Trust will be arranged in an accredited record-keeping system if created electronically and in structured paper files that enables the Trust to obtain the maximum benefit from quick and easy retrieval of information.

Where the viewing or use of a record is restricted, there must be systems in place for identifying who is authorised to view, create and use the record. These systems must be auditable.

The control over copies of records must be managed to ensure only official records are classified and maintained. These will be managed by the system Information Asset Owner.

For reasons of business efficiency, or in order to address problems with storage, consideration should be given to the option of scanning into electronic format, records which currently exist in paper format. Where scanning of documents into a digitised format takes place this must be done in accordance with the British Standards, in particular the 'Code of Practice for Legal Admissibility and Evidential Weight of Information Stored Electronically' (BIP 0008).

In order to fully realise the benefits of reduced storage requirements and business efficiency, Information Asset Owners should consider disposing of paper records which have been copied or scanned into a digital format and stored in accordance with appropriate standards.

See the Health Records Management Procedure or the Corporate Records Management Procedure for further information.

## 4.2. Record Use and maintenance

All information must be used consistently, only for the purpose for which it was intended and never for an individual employee's personal gain or purpose. If in doubt employees should seek guidance from their manager.

When information is being recorded and used, employees should ensure the Data Protection Act and Caldicott Principles are being adhered to:

Data Protection Principles

- Personal information must be fairly and lawfully processed
- Personal information must be process for limited purposes
- Personal information must be adequate, relevant and not excessive
- Personal information must be accurate and up to date
- Personal information must not be kept for longer than is necessary
- Personal information must be processed in line with the data subjects' rights
- Personal information must be secure
- Personal information must not be transferred to other counties without adequate protection

Caldicott Principles

- Justify the purpose(s)
- Don't use personal confidential data unless it is absolutely necessary
- Use the minimum necessary personal confidential data
- Access to personal confidential data should be on a strict need-to-know basis
- Everyone with access to personal confidential data should be aware of their responsibilities
- Comply with the law
- The duty to share information can be as important as the duty to protect patient confidentiality

All information needs to be maintainable through time. The qualities of availability, accessibility, interpretation and trustworthiness must be maintained for as long as the information is required, perhaps permanently, despite changes in the format.

All physical records should be tracked if they are moved from one location to another. Records should not be removed unless the appropriate tracking system has been updated. All staff are responsible for tracking records.

Where there is a need to transport or transfer records either within or outside the Trust, this will be conducted in a manner that retains the security and confidentiality of the information held within the record. Personal Identifiable Information will be protected from accidental disclosure and systems will be deployed which protect the security of the personal information.

For electronic records, maintenance must include backup and migration to new platforms to ensure continued access to readable information. Trust records must not be stored on local drives, (e.g. C: Drive or Desktop), or on home computers.

Where an email forms part of a record it should be moved from the email system to an appropriate folder on a secure shared network drive.

All records, irrespective of the medium, will be stored in a manner that is safe, clean and tidy, secure from unauthorised access and stored in an environment which meets health, safety and fire regulations.

Duplication should be avoided. Usually there is only a need to maintain one master set of records.

Records that are no longer required for active patient care or business use should be archived to a designated secondary storage area; this will be a physical area for paper records or an electronic archive for digital records. Local secondary storage archive stores must be maintained in a way where records can be easily retrieved. Retrieval from local storage should be managed by the team, department, or service administrator with responsibility for records management

Records identified for archiving offsite must be tracked. For health records this would be via the clinical information system. For corporate records a manual system of tracking what records are held offsite must be put in place. If a spreadsheet is used it must be logged on the Information Asset Register of the service.

Only the Trust approved storage contractor should be used to store records offsite.

Missing, unavailable or lost records must be reported the Datix system so that a centralised record is maintained and actions taken to trace missing records are monitored.

See the Health Records Management Procedure or the Corporate Records Management Procedure for further information.

### 4.3. Record Retention

It is a fundamental requirement that all records are retained for a minimum period of time for legal, operational, research and safety reasons. The length of time for retaining records will depend on the type of records and its importance to the Trust business function.

The Trust has adopted the retention periods set out in Appendix 3 of the Records Management Code of Practice for Health and Social Care 2016 unless there is a

specific reason for this retention period being extended. Confidentiality must be safeguarded at every stage of the records management lifecycle.

Recommended minimum retention periods should be calculated from the end of the calendar year following the last entry on the document.

See the Health Records Management Procedure or the Corporate Records Management Procedure for further information.

## 4.4. Record Appraisal

Appraisal of records for disposal or destruction involves an assessment of the record to ensure there are no reasons why the record should be retained past the retention period and, an assessment of the record creation/archive dates to provide assurance the record is outside of the retention period as stated in Appendix 3 of the Records Management Code of Practice for Health and Social Care 2016.

See the Health Records Management Procedure or the Corporate Records Management Procedure for further information.

## 4.5. Record Disposal

Disposal is the term used to cover the final action taken on records. This will be either destruction or transfer to archival storage. The disposal action is determined by the appraisal process and decision.

Under the Public Records Act, NHS records over 30 years old which have been selected for permanent preservation and which are not in current use by the creating department must be transferred to a recognised place of deposit. Within the Trust and in respect of Trust records, the approved place of deposit is the Greater Manchester County Record Office (GMCRO). The IQA Manager must be consulted before records are sent to GMCRO for permanent preservation.

A record of the destruction of records should be made when departments are destroying records. This applies to both paper and electronic records. For health records the destruction can be recorded on the tracking function of the clinical system. For all other records a record destruction form must be completed and forwarded to the IQA Manager.

Records must not be destroyed in contravention of the Trust retention schedule without prior consultation with and approval from the IQA Manager.

The Independent Inquiry into Child Sexual Abuse (IICSA), has requested that large parts of the Health and Social Care sector do not destroy any records that are, or may fall into, the remit of the inquiry.

This includes children's records and any instances of allegations or investigations or any records of an organisation where abuse has, or may have occurred.

Confidential paper records should only be destroyed by Trust approved contractors. When destroying manual patient records the tracking function on the clinical system must be updated to indicate that the records have been destroyed.

Electronic records should be fully erased from Trust servers and systems. A record of destruction should be made as with paper records. Advice and guidance on how to delete records can be obtained from IT Operations. All copies must be destroyed, including back-ups so that there is no possibility of recovering the data.

Health records held on the clinical system are currently not being deleted, and this will remain the case until guidance is issued by the Department of Health.

It is a **criminal offence** under the Freedom of Information Act to destroy or alter information that has been requested in an attempt to avoid disclosure.

If a record due for destruction is known to be the subject of a request for information or a litigation case, destruction should be delayed. If it would take an excessive amount of time and effort to extract the record from those due for destruction because the destruction process has already partially begun, then this may be taken into account when calculating whether the enquiry will extend beyond the fees limit. Once the information request is completed, the record should be retained until the complaint and appeal provisions of the Freedom of Information Act have been exhausted.

See the Health Records Management Procedure or the Corporate Records Management Procedure for further information.

## 5. Training Requirements

The online Information Governance Training Tool provides modules to assist managers and staff to be trained in relevant issues.

Clinical system training is delivered via Trust induction and supplemented by the GMMH Learning Hub.

The IQA Manager will provide ad hoc advice where the need has been highlighted.

## 6. Monitoring

It is the responsibility for all line managers to ensure that employees under their immediate control, temporary or otherwise comply with this policy.

The Trust will regularly audit its records management practices for compliance with this framework. An audit schedule will be established in order to ensure that compliance with this policy is continually monitored.
The audits will:

- Identify areas of operation that are covered by the Trust's policies and identify which procedures and/or guidance should comply to the policy;
- Follow a mechanism for adapting the policy to cover missing areas if these

are critical to the creation and use of records, and use a subsidiary development plan if there are major changes to be made;

- Set and maintain standards by implementing new procedures, including obtaining feedback where the procedures do not match the desired levels of performance; and
- Highlight where non-conformance to the procedures is occurring and suggest a tightening of controls and adjustment to related procedures.

The results of audits will be reported to the Information Governance Steering Group.

| Minimum Requirement | Frequency | Process for monitoring | Evidence | Responsible Individual(s) | Response Committee(s) |
|---|---|---|---|---|---|
| Legal obligations that apply to records | On-going | ICO updates | Policy Updates | IQA Manager | IG Steering Group |
| Process for tracking records | Annual | Dip sampling | Restore reports, audit log | IQA Manager | IG Steering Group |
| Process for creating records | Annually, ad-hoc | Audit | Audit reports, completed questionnaires | IQA Manager | IG Steering Group |
| Process for retention, disposal and destruction of records | Monthly | Records of destruction, central destruction logs, audit | Completed forms, audit reports | IQA Manager | IG Steering Group |
| Updates of Risk Register | Quarterly | DATIX risk register update at monthly IMT Dept Risk meeting | Assurance Statement to RMSG | Head of IM&T Service Delivery | RMSG |

## 7. Resource/Implementation Issues

This procedure was circulated via the Integrated Governance Department's Electronic Document Management System cascade (SharePoint) to all Trust nominated policy leads in accordance with the Trust's Policy on Policies.

## 8. Risk Issues

The Trust needs to achieve a minimum of Level 2 in Information Governance Toolkit Requirement 400, 401, 402, 404, 406, 501, 506, 507, and 601,604.

All employees need to be able to recognise what constitutes a record and the differences between a record and a document. Failure to retain and manage corporate records in line with the Records Management Code of Practice for Health & Social Care (2016), could mean that the Trust is not compliant with the Public Records Act.

## 9. Requirements, Supporting Documents and References

### 9.1. Requirements

| | |
|---|---|
| **Trust Objectives** | 6 – To achieve sustainable financial strength and be well governed |
| **CQC Regulations** | 17 – Good Governance |
| **Other** | Information Governance Toolkit for Mental Health Trusts and in particular requirements:<br>400 – Clinical Information Assurance<br>500 – Secondary Use Assurance<br>600 – Corporate Information Assurance<br>Further details available at https://www.igt.hscic.gov.uk/ |
| | Her Majesty's Government Legislation including:<br>• The Data Protection Act (1998)<br>• The Freedom of Information Act (2000)<br>• The Public Records Act (1958)<br>Further details available at:<br>http://www.legislation.gov.uk/ |
| | Records Management Code of Practice for Health & Social Care (2016)<br>https://digital.nhs.uk/data-and-information/looking-after-information/data-security-and-information-governance/codes-of-practice-for-handling-information-in-health-and-care/records-management-code-of-practice-for-health-and-social-care-2016 |

### 9.2. Supporting Documents

- Confidentiality Code of Conduct
- Confidentiality Policy
- Corporate Records Management Procedure
- Data Quality Policy
- Email and Internet Usage Policy
- Freedom of Information Policy
- Health Records Management Procedure
- Information Asset Management Policy
- Information Governance Policy
- Information Security Policy
- Information Sharing Policy
- Mobile Media Security Policy
- Pseud-anonymisation Policy
- Records Management Policy
- Safe Haven Policy

### 9.3. References

- Department of Health: Confidentiality: NHS Code of Practice. Available at: Link
- Information Governance Alliance (2016). Records Management Code of Practice for Health and Social Care 2016 (online). Available at: Link
- NHS: The Care Record Guarantee: Our guarantee for NHS care records in England. January (2011), Version 5. Available at: Link
- The Access to Health Records Act (1990) Link
- The Data Protection Act (1998) Link
- The Freedom of Information Act (2000) Link
- The Ministry of Justice and The National Archives (2009). Lord Chancellor's Code of Practice on the management of records issues under section 46 of the Freedom of Information Act 2000. Available at: Link
- The National Archives (2004). Disposal Scheduling (online) Available at: Link
- The National Archives (2010). Code of practice for archivists and records managers under Section 51(4) of the Data Protection Act. Available at: Link
- The National Archives (2010). Guide 4: Keeping records to meet corporate requirements. Available at: Link
- The National Archives (2010). Managing Digital Records without an Electronic Record Management System. Available at: Link
- The National Archives (2011). Access to NHS records transferred to places of deposit under the Public Records Act. Available at: Link
- The National Archives. Complying with the Records Management Code: Evaluation Workbook and Methodology: Sector specific guidance for records managers. Available at: Link
- The Public Records Act (1958) Link
- The National Archives: 20 Year Rule: Link

## 10. Subject Expert and Feedback

Advice and support queries in relation to this document should be sent to the author.

## 11. Review

This document will be reviewed in five years, or sooner in the light of organisational, legislative or other changes.