NHS

Greater Manchester Shared Services

Records Management Policy

Greater Manchester Shared Services

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

Best Care • Best Health • Best Value

Contents

[Type text]

Document Change History

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

Document Tracking History

Date	Ver.	Person Presenting	Area Receiving	Comments
November 2016	0.1	IG Team	GMSS IG Group	Recommend Approval by the IG Group
January 2017	0.2	G Coxon	FPG	Recommend Approval after some amendments
January 2017	0.3	K Rigden	SMT	Amendments needed
February 2017	0.4	K Rigden	SMT	Final Ratification

1. Introduction and Aims

The purpose of this document is to provide guidance to all Greater Manchester Shared Services (henceforth referred to as “GMSS”) staff on Records Management. This policy is adopted from the NHS England Policy of the same name.

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 their lifecycle to their eventual disposal.

The Records Management: NHS Code of Practice for Health & Social Care 2016 has been published by the Department of Health as a guide to the required standards of practice in the management of records for those who work within or under contract to NHS organisations in England. It is based on current legal requirements and professional best practice.

GMSS records are its corporate memory, providing evidence of actions and decisions and representing a vital asset to support daily functions and operations. Records support policy formation and managerial decision- making, protect the interests of the NHS and the rights of patients, staff and members of the public. They support consistency, continuity, efficiency and productivity and help deliver services in consistent and equitable ways.

For the purpose of this document GMSS records refer to Corporate records (i.e. personnel files, minutes etc.) and clinical/health records (patient health records) where appropriate.

GMSS has adopted this records management policy and is committed to on-going improvement of its records management functions as it believes that it will gain a number of organisational benefits from so doing. These include:

Better use of physical and server space;
Better use of staff time;
Improved control of valuable information resources;
Compliance with legislation and standards; and
Reduced costs.

GMSS also believes that its internal management processes will be improved by the greater availability of information that will accrue by the recognition of records management as a corporate function.

The development of these procedures and practices will help the organisation meet the required standards ensuring that records are managed and controlled appropriately throughout their life cycle, in the most cost effective way, and in accordance with legal, operational and information needs.

It is the responsibility of all staff including those on temporary or honorary contracts, agency staff and students to comply with this policy.

The aims of this policy are to ensure that:

- records are available when needed - from which GMSS is able to form a reconstruction of activities or events that have taken place;
- records can be accessed - records and the information within them can be located and displayed in a way consistent with its initial use, and that the current version is identified where multiple versions exist;
- records can be interpreted - the context of the record can be interpreted: who created or added to the record and when, during which business process, and how the record is related to other records;
- records can be badged with a GMSS logo – the record reliably represents the information that was actually used in, or created by, the business process, and its integrity and authenticity can be demonstrated;
- records can be maintained through time – the qualities of availability, accessibility, interpretation and GMSS worthiness can be maintained for as long as the record is needed, perhaps permanently, despite changes of format;
- 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; and

- staff are trained - so that all staff are made aware of their responsibilities for record-keeping and record management.

2. Scope

This policy applies to those members of staff that are directly employed by GMSS and for whom GMSS has legal responsibility including agency and interim staff. For those staff covered by a letter of authority/honorary contract or work experience the organisation's policies are also applicable whilst undertaking duties for or on behalf of GMSS. Further, this policy applies to all third parties and others authorised to undertake work on behalf of GMSS.

This guidance relates to all clinical and non-clinical records held in any format by GMSS, or any party on behalf of GMSS. A record is anything which contains information (in any media) which has been created or gathered as a result of any aspect of the work of NHS employees, including:

- administrative records including e.g. personnel, estates, financial and accounting records: notes associated with complaint-handling;
- audio and videotapes, cassettes and CD-ROMs;
- computer databases, output, and disks, and all other electronic records;
- material intended for short term or transitory use, including notes and "spare copies" of documents;
- meeting papers, agendas, formal and meetings including notes taken by individuals in note books and bullet points are all subject to the above; and
- emails and other electronic communications.

The above list is not exhaustive.

Limitations and Applications for GMSS Staff

The Introduction of the Health and Social Care Act 2012 removed some of the powers and rights GMSS had to obtain, handle, use and share confidential and identifiable information from GMSS. In general, GMSS staff are not entitled to use Personal Confidential Data (PCD). Whilst this policy references health records, this advice is only applicable to GMSS staff who have a legal right to this information, and is not applicable to all staff.

Further information on the above is available in GMSS Staff IG Handbook and the Information Governance and Data Protection Policies.

3. Definitions

Records Management is 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 organisations and preserving an appropriate historical record. The key components of records management are:

- Record creation;

- record keeping;
- record maintenance (including tracking of record movements);
- access and disclosure;
- closure and transfer;
- appraisal;
- archiving; and
- disposal.

In this policy, **Records** are defined as 'recorded information, in any form, created or received and maintained by the organisations in the transaction of its business or conduct of affairs and kept as evidence of such activity.'

Information is a corporate asset. The Records are important sources of administrative, evidential and historical information. They are vital to the organisation 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. All information should be recorded on GMSS Information Asset Register.

The term **Records Life Cycle** describes 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.

Corporate/business records are defined as anything that contains information in any media, which has been created or gathered as evidence of undertaking of work activities in the conduct of business. Corporate records may also be generated through supporting patient care and can also be generated through agency/casual staff, consultants and external contractors.

Corporate records types include;

- Administrative records (including personnel, estates, financial and accounting, contract records , litigation and records associated with complaints- handling)
- Registers and rotas
- Office /appointment diaries
- Photographs, slides, plans or other graphic work (not clinical in nature)
- Micro film a (i.e. fiche/film)
- Audio and video tapes
- Records in all electronic formats including emails

A health record is defined as being any 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 the individual.

4. NHS Number

The NHS Number is a unique number given to every baby born in England and patient registered with the NHS and is the prime patient identifier. The patient identifier enables administrative records to be exchanged more safely between both electronic and manual systems.

GMSS will ensure that NHS numbers are used on all clinical communications, clinical records and on all systems processing patient information.

And will further ensure the following principals are applied when processing patient information and will not procure any IT system that does not support these principals.

NHS Number Principals

Find It

- Find / Request the NHS Number on referral letters / forms received;
- Determine and verify the NHS Number before or at the start of an episode of care;
- If this is not possible then tracing should be performed as early as possible in the episode either at point of contact or as a back office process.

Use It

- Use the NHS Number to search for an electronic record as the 'First Choice';
- Use the NHS Number to identify people presenting for care;
- Include the NHS Number on electronic records, wristbands, notes, forms, letters, document and reports which include patient information and are used for that person's care;
- Use the NHS Number as the key identifier for service users;
- Ensure systems can support the NHS Number;
- Use the Personal Demographics Service (PDS) or Demographics Batch Service (DBS) to trace NHS Numbers;

Share It

- Include in all communications, written, verbal and electronic, during telephone calls, on all letters, referrals, forms, documents;
- Internally within your organisation and with all other organisations you contact as part of the provision of care;
- Ensure the NHS Number is included when providing users with any letters or forms;
- Supply the NHS Number as the key identifier for any patient information that assess across systems and organisation boundaries

5 Roles and Responsibilities

Managing Director

Overall accountability for records management across the organisation lies with the Managing Director who has overall responsibility for establishing and maintaining an effective document management system, for meeting all statutory requirements and adhering to guidance issued in respect of procedural documents.

Caldicott Guardian

GMSS Caldicott Guardian is the conscience of the organisation and IS responsible for ensuring that national and local guidelines on the handling of confidential personal CLINICAL information are applied consistently across the organisation. They are responsible for ensuring patient identifiable information is shared in an appropriate and secure manner

Senior Information Risk Owner (SIRO)

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

Information Asset Owners (IAOs)/Administrators (IAAs)

Under the responsibility of the SIRO:

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

Information Governance Lead

Overall responsibility for the Records Management Policy and implementation lies with GMSS Information Governance Manager who has delegated responsibility for managing the development and implementation of records management procedural documents and for working with GMSS Information Governance Team.

GMSS Information Governance Lead is responsible for co-ordinating, publicising, implementing and monitoring the records management processes and reporting issues or concerns to the IG Group.

Senior Managers/Information Asset Owners

Senior managers and Information Asset Owners are responsible for the quality of records management within GMSS and all line managers must ensure that their staff, whether administrative or clinical, are adequately trained and apply the appropriate guidelines, that is, they must have an up-to-date knowledge of the laws and guidelines concerning confidentiality and data protection.

All Staff

All GMSS employees (including temporary and contract staff), whether clinical or administrative, who create, receive and use records in any form of media have records management responsibilities. In particular all staff must ensure they keep appropriate records of their work in GMSS and manage those records in keeping with this policy and with any guidance. Furthermore, any record that any individual creates is a public record and may be subject to both legal and professional obligations, including compliance with relevant legislation included the Freedom of Information Act and the Data Protection Act.

This responsibility is established at, and defined by, the law (Public Records Act 1958). Furthermore, as an employee of the NHS, any records created by an employee are public records.

Staff handling personal confidential information must remember they have a common law duty of confidence to patients and other employees and a duty to maintain professional ethical standards of confidentiality.

6 Registration of Record Collections

GMSS will establish and maintain mechanisms through which departments and other units can register the records they are maintaining. The Information Asset Registers will facilitate:

- The classification of records into series : and
- The recording of the responsibility of the individuals creating records.

7 Record Creation.

GMSS should have a process for documenting its activities, taking into account the legislative and regulatory environment in which it operates.

Records must hold adequate 'integrity' so their evidential weight is legally admissible, and can withstand scrutiny in the event of litigation or claim. True and accurate records protect the right of the individual or GMSS.

All records should be complete and accurate:

- To allow staff to undertake appropriate actions in the context of their responsibilities;
- to protect legal and other rights of the organisation, patients, staff and other people affected;
- to show proof of validity and authenticity.

Records should be created and maintained in a manner that ensures that they are clearly identifiable, accessible, and retrievable in order to be available when required. All records should have a unique number or filling system, which will be applicable only to that record. For example, a patient's medical record will be identifiable by the NHS number and an employee's personal file held in personnel number. Records must have clear and precise formats and must be structured in the same way that files of the same description are structured with an easy to follow standard index, either numerical, by date or alphabetically.

The following should be documented when a paper or electronic record is created:

- File reference;
- file title;
- if appropriate protective marking i.e. NHS Protect or NHS Confidential;
- if possible an anticipated disposal date and what action to take;
- where action cannot be anticipated, mechanisms must be in place to ensure this action takes place when the file is closed;
- all filling systems to be documented and kept up to date.

Managers of departments should ensure staff are made aware of their responsibilities, are properly trained and that reviews and monitoring for compliance are undertaken.

All major decisions or key actions which may result from discussions or meetings should be recorded as this provides key evidence of business of business decision making activity.

GMSS will ensure consistency is established in the way information is presented to target audiences, both internally and externally. When creating a record GMSS will need to achieve the following:

Hold the necessary records to enable staff to perform their duties;

- ensure information can be located promptly and time wasted on locating or recreating lost documents reduced;
- appropriate disclosure of information to staff or the public who require and are authorised to access;
- evidence of individual and corporate performance and activity;
- physical and digital space is used effectively;
- records created are able to meet GMSS legal obligations;
- organizations can preserve its corporate memory and track business decisions or transactions over time.

For checklist on how to create a Record refer to Appendix 1, Checklist; Creating a Record.

8 Record Quality

All GMSS staff should be fully trained in record creation use and maintenance, consummate to their roles, including having an understanding of what should be recorded and how it should be recorded and the reasons for recording it. Staff should know:

- How to validate the information with the patient or the carer or other records to ensure they are recording the correct data;
- why they are recording it;
- how to identify, report and correct errors;
- the use of the information and record;
- what records are used for and the importance of timeliness, accuracy and completeness;
- how to update and add information from other sources.

Full and accurate records must possess the following three essential characteristics:

- Content – the information it contains (text, data, symbols, numeric, images or sound);
- Structure – appearance and arrangement of the content (style, font, page and paragraph breaks, links and other editoral devices).
- Context – background information that enhances understanding of the business environment/s to which the records relate (e.g. metadata, software) and the origin

(e.g. address title, function or activity, organisation, program or department).

The structure and context of each record will alter depending on the record being created. For example, policies will need to hold contextual information like author names, review date and ratification information; whereas agenda does not require that type of information but should include attendees, venue, date and time.

Quality Checking

GMSS should establish quality checks which will minimise/eradicate errors. A different member of staff should quality check to the one that has input the information. Dependent on the type of record the following checks should be undertaken:

- Ensure the correct retention period has been input onto the document which confirms the right retention/destruction will have been calculated;
- ensure all names are spelt correctly and in the correct format;
- ensure the unique identifiers are correct and in the right format;
- check the barcode number is correct (if relevant);
- the inventory should be checked for all other possible errors.

For further information on how to check the quality of a record refer to
Appendix 2 – Quality of Record entries.

9 Record Keeping

Implementing and maintaining an effective records management service depends on knowledge of what records are held, where they are stored, who manages them, in what format(s) they are made accessible, and their relationship to organisational functions. An information inventory or record audit is essential to meeting this requirement. The inventory will help to enhance control over the records, and provide valuable data for developing records appraisal and disposal policies and procedures.

Paper and electronic keeping systems should contain descriptive and technical documentation to enable the system to be operated efficiently and the records held in the system to be understood. The documentation should provide an administrative context for effective management of the records.

All records must conform to these record keeping guidelines, legislation, NHSLA, DoH, Information Governance requirements and professional guidelines.

10 Record Maintenance

The movement and location of records should be controlled to ensure that a record can be easily retrieved at any time, that any outstanding issues can be dealt with, and that there is an auditable trail of record transactions.

Storage accommodation for current records should be clean and tidy, should prevent damage to the records and should provide a safe working environment for staff.

For records in digital format, maintenance in terms of back-up and planned migration to new platforms should be designed and scheduled to ensure continuing access to readable information.

Equipment used to store current records on all types of media should provide storage that is safe and secure from unauthorised access and which meets health and safety and fire regulations, but which also allow maximum accessibility of the information commensurate with its frequency of use.

When paper records are no longer required for the conduct of current business, their placement in a designated secondary storage area may be a more economical and efficient way to store them. Procedures for handling records should take full account of the need to preserve important information and keep it confidential and secure. Archiving policies and procedures should be observed for both paper and electronic records.

All individual files should be weeded on a regular basis, to ensure the key documentation is readily identifiable and accessible. Bulky files should contain no more than 4 years' worth of records. Any file older than this should be culled and removed to an inactive file. The front cover of each such volume must clearly indicate that other volumes exist.

Any duplicate documents (except where copy letters sent or received have had comments added by hand) should be culled and confidentially destroyed.

In order to identify when records were last active or the service user was last in contact with the service, it is advisable that year labels are used on the front cover.

If there are separate sets of records relating to the same service user which is a consequence of historic practice, these should all be stored together upon discharge and kept together when archived.

A contingency or business continuity plan should be in place to provide protection for all types of records that are vital to the continued functioning of the organisation.

11 Tracking of Records.

Accurate recording and knowledge of the whereabouts of all clinical and non-clinical records is essential if the information they contain is to be located quickly and efficiently. Records must not be taken out of the office unless this has been agreed by the Line Manager and a tracking mechanism is in place. The tracking system could be manual or electronic and linked to a department's IT system.

Tracking mechanisms should record the following (minimum) information:

- The item reference number of the record or other identifier;
- a description of the item (e.g. file title);
- the person, unit or department, or place to whom it is being sent;
- the date of the transfer to them;
- the date of the information returned (if applicable).

Manually operated tracking systems are common methods for manually tracking the movements of active records and include the use of:

- A paper register – a book, diary, or index card to record transfers, item reference number of the record or other identifier;
- file "on loan" (library type) cards for each absent file, held in alphabetical or numeric order;

- file “absence” or “tracer” cards put in place of absent files.

Electronically operated tracking systems include:

- A computer database, excel spread sheet in place of paper/card index;
- bar code labels and readers linked to computers;
- work flow software to electronically track documents.

The minimum data which needs to be recorded includes:

- service user’s name;
- NHS number;
- date the records were removed,;
- destination and name of intended recipient;
- name of the person releasing the records.

A well thought out, manual or electronic system should:

- provide an up-to-date easily accessible movement history and audit trail;
- be routinely checked and updated;
- be recorded i.e. all movements of a record even if the record is exchanged between teams/staff members within the same building;
- provide a return receipt and it made clear to whom the records should be returned ;
- ensure information recorded on the tracking system must be correct and applicable to ensure the system remains effective;

- take into consideration any filing that comes in whilst the records are traced out and must be filed according to local documented procedures until such time as the records are returned;
- ensure that any records are returned safely to their correct home and absent records are chased on a frequent basis;
- maintain a log of all records received into the department including the date received, service user name and NHS number.

Managers should ensure that training and procedures are in place for manual and electronic tracking systems and that they are being adhered to.

12 Record Transportation.

All GMSS employees and contractors have a legal duty to keep information safe and secure. Security and confidentiality of records should be paramount at all times. This is particularly important, in high security risk situations such as the transportation of records between sites. Records should not be taken off site without the authorisation of the relevant line manager. To reduce the risk of loss of records and the risk of breaches of confidentiality staff are advised to observe the following minimum precautions:

- Records should be tracked out of the respective department so that other staff are aware of the location of the record;
- records should never be left unattended where it would be possible for an unauthorised person to have access to them;
- records being transported should always be kept out of sight;
- if records are taken home, they must be stored securely in accordance with the staff members Professional Code of Conduct.

NHS organisations are required to map their information flows in accordance with the guidance in the Information Mapping Tool. The objective of this is to demonstrate that an organisation, in this case GMSS, clearly identifies and has addressed the risks associated with the transfer of identifiable information. This mapping requires all organisations to have an up to date register of information transfers (i.e. audit or map the flows of information in and out across the organisation).

Offsite movement of records or other confidential/sensitive information.

Security requirements also apply when staff records are transported. It is recognised that staff may find it necessary to remove records from their base, to ensure business continuity. To reduce the risk of loss of such records and to reduce the risk of breaches of confidentiality there are various considerations to be made, based on best practice:

- Records should not be removed for administrative purposes i.e. writing reports. A trace should be kept at the base from which records have been removed and staff are aware of the location of the record;
- Records should not be left unattended in cars;
- Records kept in any staff possession should remain safe and secure at all times i.e. out of sight and locked away when not in use;
- Records should only be taken off site with the approval of the Line Manager. If a record is taken off site, it must be stored securely in accordance with the Confidentiality Code of Conduct – Guidelines for Staff;
- Any vehicle used for the transportation of records must be insured for business use. If the staff member is involved in a road traffic accident which necessitates the car being left on the roadside or taken to a garage, records should be removed.
- If this is not possible the matter should be reported to the Line Manager and an incident form completed.

Appendix 3 – Transportation of information log sheet. This should be used when transporting any records from one place/organisation/department to another.

For information and procedures on posting records/sensitive information refer to Appendix 5.

13 Lost/Missing Records

A lost/missing record is a record either that cannot be found following a search in the office environment or is unavailable.

The loss of records constitutes a reportable incident and should be reported in accordance with GMSS Incident Reporting Policy.

It is importance that records can be retrieved at any time during the retention period, whether for management or legal purposes.

14 Scanning

For reasons of business efficiency and in order to alleviate storage space/issues, GMSS can scan into electronic format inactive records which exist in paper format. The following factors should be taken into account:

- the costs of the initial and then any later media conversion to the required standard, bearing in mind the length of the retention period for which the records are required to be kept;
- the need to consult in advance with the local Place of Deposit or The National Archives with regard to records which may have archival value, as the value may include the format in which it was created; and
- the need to protect the evidential value of the record by copying and storing the record in accordance with 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, GMSS will securely dispose of the paper records that have been copied into electronic format and stored in accordance with appropriate standards.

15 Disclosure and Transfer of Records.

There are a range of statutory provisions that limit, prohibit or set conditions in respect of the disclosure of records to third parties, and similarly, a range of provisions that require or permit disclosure. Guidance should be sought from the Information Governance Team prior to any disclosure. If the request for access to information is made under the Freedom of Information Act 2000, then the request should immediately be forwarded to the Patient Services Department within the Greater Manchester Shared Services in order to comply with the deadlines specified in the Act.

The Caldicott Guardian should be made aware of any proposed disclosure of confidential patient information, informed by the Department of Health publication Confidentiality: NHS Code of Practice.

The mechanisms for transferring records from one organisation to another should also be tailored to the sensitivity of the material contained within the records and the media on which they are held. The Information Governance Lead can advise on appropriate safeguards.

16 Retention, Archiving and Disposal of Records

Appraisal refers to the process of determining whether records are worthy of additional retention or permanent archival preservation. If the latter, this should be undertaken in consultation with the National Archives, or with an approved Place of Deposit where there is an existing relationship.

The purpose of the appraisal process is to ensure that the records are examined at the appropriate time to determine whether or not they are worthy of archival preservation, whether they need to be retained for a longer period as they are still in use, or whether they should be destroyed.

The procedure for recording the disposal decisions made following appraisal must be followed. GMSS will determine the most appropriate person(s) to carry out the appraisal in accordance with the retention schedule. This should be a senior manager with appropriate training and experience who has an understanding of the operational area to which the record relates.

Most NHS records, even administrative ones, contain sensitive or confidential information. It is therefore vital that confidentiality is safeguarded at every stage of the lifecycle of the record, including destruction, and that the method used to destroy such records is fully effective and ensures their complete illegibility.

17 Record Closure

Records should be closed (i.e. made inactive and transferred to secondary storage) as soon as they have ceased to be in active use other than for reference purposes. Each year a list of records coming to the end of their retention period should be reviewed. An indication that a file of paper records or folder of electronic records has been closed, together with the date of closure, should be shown on the record itself as well as noted in the index or database of the files/folders. Where possible, information on the intended disposal of electronic records should be included in the metadata when the record is created.

Records/information contain personal confidential information and it is therefore vital that confidentiality is safeguarded at every stage and that the method used to destroy records is fully effective and complete illegibility is secured. Destruction of all records, regardless of the media in which they are held should be conducted in a secure manner ensuring safeguards are in place against accidental loss or disclosure.

18 Retention Schedules and Record Disposal

It is a fundamental requirement that all of GMSS 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 record and its importance to GMSS's business functions.

GMSS has adopted the retention periods set out in the Records Management: NHS Code of Practice for Health and Social Care 2016. These retention schedules outline the recommended minimum retention period for NHS records.

Senior Managers will be responsible for ensuring disposal schedules are implemented as part of a rolling programme. Recommended minimum retention periods should be calculated from the end of the calendar year following the last entry to the document. i.e. a file's first entry is in February 2001 and the last December 2006, the minimum retention period is eight years, it should therefore be kept in its entirety at least until 31st December 2014. If a member of staff feels that a particular record needs to be kept for longer than the recommended minimum period or there is a specific purpose further advice and approval should be sought from the Service Senior Manager/Director.

Where there are records held by the organisation that do not have a retention period advice should be sought from the Information Governance Group where approval and inclusion of the retention period will be granted.

Records selected for archival preservation and no longer in regular use by the organisation should be transferred as soon as possible to an archival institution that has adequate storage and access facilities. Non-active records should be transferred no later than 30 years from creation of the record, as required by the Public Records Act.

Records not selected for archival preservation and which have reached the end of their administrative life should be destroyed in as secure a manner as is appropriate to the level of confidentiality or protective markings they bear.

The methods used throughout the destruction process must provide adequate safeguards against the accidental loss or disclosure of the contents of the records. Contractors, if used, are required to sign confidentiality undertakings and to produce written certification as proof of destruction.

A record of the destruction of records, showing their reference, description and date of destruction should be maintained and preserved by GMSS, thus making GMSS aware of any destroyed records.

If a record due for destruction is the subject of a statutory request for information or potential legal action, destruction should be delayed until disclosure has taken place or the legal process complete. Advice should be obtained from the Information Governance Lead.

It must be remembered that the destruction of records is an irreversible act.

Please see Appendix 7 - Retention Schedule for further details

19 Subject Access Request

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

Any individual is entitled to:

- Know what information is held about them and why;
- gain access to it regardless which media it is held in;
- have their information kept up to date;
- require GMSS rectify / block, erase or destroy inaccurate information;
- not have processed confidential information about them likely to cause damage or distress;
- not have processed confidential information about them for the purposes of direct marketing.

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

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

Formal requests to GMSS for access to records, summaries and reports should be made in writing to:

Information Governance Service
Greater Manchester Shared Services
Ellen House
Oldham
OL9 6EE

GMSS will only be able to action requests for their own employees, should they wish to access information held about them in their personnel files or any other information.

Where GMSS receive requests for health records they should be passed onto the relevant NHS organisation (hospital CCG, GP practice), and the individual/requester will be notified of the action taken.

GMSS is not obliged to comply with an individual's request unless it is satisfied as to the identity of the person making the request and their right to do so.

Formal requests should contain the following information:

- Sufficient information to enable the identification and location of the information being requested;
- information to prove the identity of the applicant, or the nature of business for the information is requested;
- a valid consent from the individual themselves or if a child those with parental responsibility are given access;
- a person who has been granted power of attorney or an agent by the courts.

Where a child is considered capable of making decisions about his/her medical treatment the consent of the child must be sought before a person with parental responsibility is given access.

It is important to note that letter, fax and email requests all constitute formal written requests.

In some cases, the individual may wish to view their record instead of receiving a copy. Requests to view should be made in the same way as requests for copies.

In a clinical setting if a health professional is asked informally by the patient during a consultation if they can view their records then and there, that health professional (the record holder) can share their own professional information with that patient /client (under their care) with or without first consulting their manager.

Informal requests to access a health records while the patient/client is still receiving care is therefore encouraged, following good practice advice around the management of records and documentation.

Who can make a request?

Patients and staff who wish to see what is written about them in their records have a legal right to do so subject to given exemptions, as prescriber by the Data Protection Act 1998 (DPA).

Requests for access to records are usually for health records and are made by:

- A patient directly;
- a patients representative;
- a solicitor requesting records in respect of a claim against another party;
- a solicitor acting either to investigate or notify a claim against GMSS;
- Children or family Court Advisory Support Service (CAFCASS) – for reports (not records);
- Criminal Injuries Compensation Authority (CICA) – for medical information (or records);
- Department of Social Security (DSS) or Department of Work and Pensions (DPP);
- the Police, who may request access under the Crime and Disorder Act 1998;
- a Court Order (for e.g. for access under the Civil Procedure Rules, the Data Protection Act 1998;
- Coroner's Office.

Responding to requests.

Any requests for access to records made to GMSS should be sent onto the Information Governance Team who will forward onto the correct party as soon as possible. GMSS should inform the individual/requester what has happened to the request i.e. sent onto relevant party to handle.

Any requests for access to staff records to GMSS should be sent onto the Information Governance Team who will liaise with the relevant department, following the Subject Access Procedure.

20 Risk Management.

Information security incidents may take many forms including the following:

- Unauthorised access to a building or areas containing confidential information;
- car theft/break-ins to on-call staff carrying individual records;
- authorised access which is misused (staff);
- electronic access (hacking) and viruses;
- unauthorised access to records away from premises (e.g. laptops and notes etc.);
- loss of identifiable / sensitive information.

Incident or near misses relating to a breach in the security regarding the use, storage, transportation or handling of records must be reported **immediately** using GMSS incident Reporting Form. This increases the possibility of recovering lost records and ensuring continuity of service/healthcare.

A lost record is defined as a record that cannot be located within 5 working days of first attempt to access the record or a record that has been stolen from a known place, for example the boot of a car. Appendix 4 provides a procedure that GMSS Staff should follow such they find themselves involved in such an incident.

In the event a record may have been stolen or lost and therefore have the potential to get into the public domain, GMSS has a responsibility to inform the individual providing an explanation of what GMSS is doing to recover the notes (if necessary) and what measures will be taken to prevent a reoccurrence.

Where records have been inadvertently mislaid and/or destroyed a temporary folder should be created which should hold the latest documentation until such a time that this can be transferred/merged with the original records.

Further advice on GMSS Incident Reporting process is available from the Risk Manager.

21 Records Management and System Audit.

The process for monitoring and evaluating the effectiveness of this policy, including obtaining evidence of compliance will be part of the Information Governance annual self-assessment audit process (IG Toolkit). GMSS will regularly audit its records management practices for compliance with the framework.

The audit will:

- Identify areas of operation that are covered by GMSS 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 related procedures.

The results of audits will be reported to the relevant quality and standards groups within GMSS under designated authority from GMSS Governing Body.

22 IG Training and Awareness.

Information Governance training must be undertaken on an annual basis. GMSS staff are mandated to undertake the mandatory Information Governance e-learning module annually. Records Management features in this training. All GMSS Staff will be made aware of their responsibilities for record-keeping and record management.

Where staff may take on a specific Information Governance roles within GMSS e.g. Records Manager, additional Information Governance training will be required. For further guidance refer to GMSS Training Needs and Analysis (TNA) Document.

The online Information Governance Training Tool modules will be utilised and uptake will be monitored. Where necessary GMSS can request ad-hoc face to face training sessions relating to Records Management this will be co-ordinated by GMSS Information Governance Team.

GMSS Information Governance Group will be responsible for ensuring that this policy is implemented, and that the records management system and processes are developed, co-ordinated and monitored.

This policy will be placed on GMSS Intranet for all staff to access.

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

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

23 Monitoring and Review.

This policy will be reviewed on an annual basis, and in accordance with the following as and when required:

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

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

24 Legislation and Related Documents.

All NHS records are public records under the Public Records Acts. GMSS will take actions as necessary to comply with the legal and professional obligations set out in the Records Management: NHS Code of Practice for Health & Social Care 2016, in particular:

- The Public Records Act 1958;
- The Data Protection Act 1998;
- The Freedom of Information Act 2000;
- The Common Law Duty of Confidentiality; and
- The NHS Confidentiality Code of Practice
- National Archive - http://www.nationalarchives.gov.uk/

This Policy should be read in conjunction with GMSS IG Policies:

GMSS will also take action to comply with any new legislation affecting records management as it arises.

Appendix 1 Checklist: Creating a Record.

- □ Check you know how to create adequate records and what information they should contain
- □ Follow relevant GMSS policies and guidelines to ensure creating full and accurate records
- □ Establish and document local procedures on creating business critical records to the department, or if using a corporate or local proforma; and ensure procedures are followed
- □ Use corporate templates wherever available so it clearly identifies the nature of the information and type of document
- □ Include fundamental elements like author, date, title, department, contact details, and it holds the approved corporate identity
- □ Ensure documents hold the relevant information specifically required for that type of record, like in the case of policies or forms. In the example of a policy this would include: executive signature, approval route, review date, EIA if applicable
- □ Capture decision-making in minutes or when creating records or emails, and that you maintain a record of any transactions. For example, agreements or discussions that impact on your work or with other teams/organisations
- □ Always ensure that the information you are recording is accurate and objective
- □ Use standard terms to describe documents and be consistent with use of acronyms
- □ Identify the creator and use their job title, plus other people who may have contributed to the document
- □ Explain within the text of the document, any codes or abbreviations used, as their meaning may become less clear over time
- □ Do not use logos, icons or catchphrases on documents that have been formally approved; include GMSS logo in all appropriate records
- □ Remember that your records, or local record keeping practises may be required for performance checks or in the invent of a claim or litigation

Appendix 2 – Quality of Record Entries

Good record keeping is a mark of skilled and safe practice, whilst careless or incomplete record keeping often highlights wider problems with individual practice.

Structure and Content of Records

Where possible there must be one set of records for each data subject/individual.

Unique Identifier

A unique identifier must be used to ensure that records can be retrieved when archived or stored.

Record entries should be:

- Complete
- Legible
- Contemporaneous, i.e. written as soon as possible
- Consecutive
- If appropriate, signed by the data subject/individual according to the service specific policies
- Only in exceptional circumstances, should entries to records be delayed

Abbreviations

Abbreviations must not be used routinely.

Alterations

Contemporaneous alterations to records are acceptable when an entry has been made in error. When this occurs, the author must take the following actions:

- Make an entry stating "written in error" near the incorrect entry
- Sign, date and record the time of the annotation making the change
- Strike through the original entry with a single line leaving it discernible
- Make the correct entry, signing it and dating it

It is unacceptable to:

- Delete or erase notes, such that the entry is no longer legible
- Use correction fluids of any part of a clinical record
- Change original entries, other than as specified above
- Change entries made by another person

Appendix 3 – Transportation of information log sheet

Address for Reply
Direct Telephone Number:
Direct Fax Number:
E-Mail Address:

Description of information to be transported / list of records, folders or disc titles:
………
………
………
………
………

Number of records / folders / discs / items:
…………………………………………………………………

To be transported by:
Name (Print):
…………………………………………..

Organization and Designation:
…………………………………………..

Contact Number:
…………………………………………...

To be received by:
Name (Print):
…………………………………………..

Designation:
……………………………………………………………………………………………..

Organization name and Address:
…………………………………………………………………………

(including postcode)
…………………………………………………………………………………………...

Method of transportation:
……………………………………………………………………………………

Estimated duration of transit:
……………………………………………………………………………….

Goods received by Courier/Organization/Department:

[Type text]

Date: ……………………………. Time: ……………..
Print Name: ……………………….

Signature: ....

Name of GMSS employee handing over the information:
………………………………………………....

Designation:
……………………………………………………………………………………………..

Contact Number:
……………………………………………………………………………………………..

Signature: Time and Date:
……………………………………………………………………………..

Goods received by: Date: …………………….......... Time: ………………………………………

Print Name: ……………………….Signature: ……………………………………………………………

The receiver (courier/organization/department etc.) will immediately contact GMSS using the above contact details to confirm that the information has been successfully delivered. A copy of this form may be provided to the receiver on request.

[Type text]

Appendix 4 – Procedure for handling Missing/Lost Records

Lost records

- The member of staff should report the missing record to his/her supervisor/ manager as soon as possible
- The supervisor/manager should ensure that a thorough search takes place, using tracking methods, including initiating a search at the base where the record should be kept
- The event must be entered in the Missing Record Log and in addition an Incident Form completed and forwarded to the Risk Manager
- A temporary record should be created, clearly marked as a temporary record, populated with all relevant information available for that data subject/individual. A temporary record should be set up and tracked on the relevant systems for the Department
- When original records are located the missing record log should be updated with details of where/how the original was located, and the two folders should be merged

Unavailable/Missing records

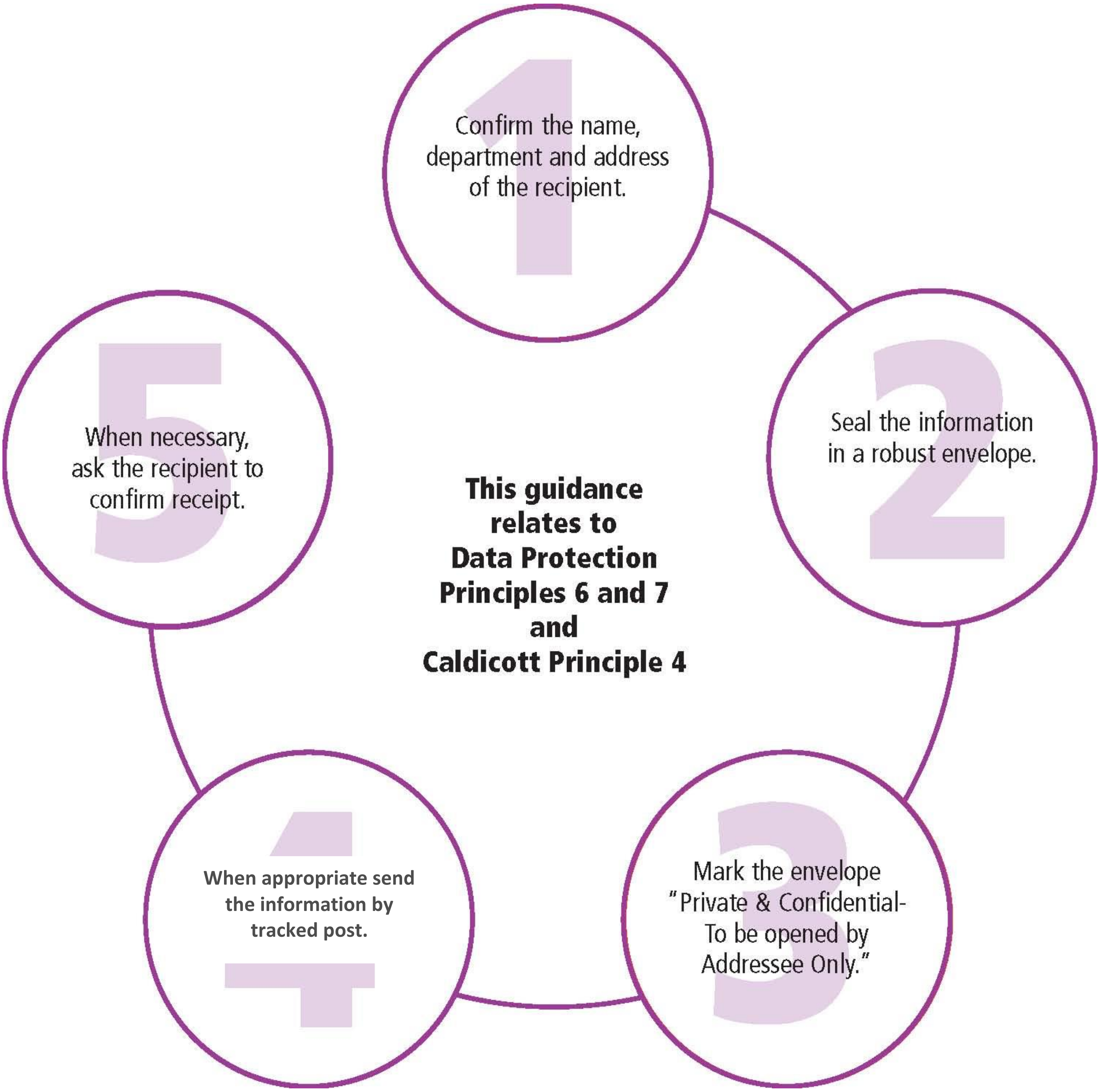
- A record is regarded as unavailable if it is in use elsewhere and/or cannot be retrieved in time for an appointment
- An entry should be made in the Missing Records Log
- A temporary record should be created, as described in the above section
- If an appointment is deferred (i.e. individual has a meeting/appointment with HR) as the record is not available this should also be recorded in the Missing Record Log

Reasons for records being unavailable may include:

- Record needed for another appointment/meeting
- Record with another Team/ Department
- Record not tracked
- Misfiled
- Wrong record/volume/temp record(s) sent

Appendix 5 – Sending Information via Postal Service

Guidance for sharing Personal, Confidential or Sensitive information by POST



1. Confirm the name, department and address of the recipient.
2. Seal the information in a robust envelope.
3. Mark the envelope "Private & Confidential- To be opened by Addressee Only."
4. When appropriate send the information by tracked post.
5. When necessary, ask the recipient to confirm receipt.

This guidance relates to Data Protection Principles 6 and 7 and Caldicott Principle 4

Appendix 6 – Corporate Documents List

Full Guidance and retention schedules can be found here: **http://systems.digital.nhs.uk/infogov/iga/rmcop16718.pdf**

The new retention schedule – lists records under the following categories – see appendix 3 of the above link for further details.

Care records - Std
Care records – Non Std
Pharmacy
Pathology
Event & Transaction Records
Telephony Systems
Births Deaths & Adoption Records
Clinical Trials & Research
Corporate Governance
Communications
Staff Records
Procurement
Estates
Finance
Legal, Complaints and Information Rights

Record Type	Retention start	Retention period	Action at end of retention period	Notes
9. Corporate Governance				
Board Meetings	Creation	Before 20 years but as soon as practically possible	Transfer to a Place of Deposit	
Board Meetings (Closed Boards)	Creation	May retain for 20 years	Transfer to a Place of Deposit	Although they may contain confidential or sensitive material they are still a public record and must be transferred at 20 years with any FOI exemptions noted or duty of confidence indicated.
Chief Executive records	Creation	May retain for 20 years	Transfer to a Place of Deposit	This may include emails and correspondence where they are not already included in the board papers and they are considered to be of archival interest.
Committees Listed in the Scheme of Delegation or that report into the Board and major projects	Creation	Before 20 years but as soon as practically possible	Transfer to a Place of Deposit	
Committees/ Groups / Sub-committees not listed in the scheme of delegation	Creation	6 Years	Review and if no longer needed destroy	Includes minor meetings/projects and departmental business meetings

[Type text]

Destruction Certificates or Electronic Metadata destruction stub or record of information held on destroyed physical media	Destruction of record or information	20 Years	Consider Transfer to a Place of Deposit and if no longer needed to destroy	The Public Records Act 1958 limits the holding of records to 20 years unless there is an instrument issued by the Minister with responsibility for administering the Act. If records are not excluded by such an instrument they must either be transferred to a Place of Deposit as a public record or destroyed 20 years after the record has been closed.

Record Type	Retention start	Retention period	Action at end of retention period	Notes
10. Communications				
Intranet site	Creation	6 years	Review and consider transfer to a Place of Deposit	
Patient information leaflets	End of use	6 years	Review and consider transfer to a Place of Deposit	
Press releases and important internal communications	Release Date	6 years	Review and consider transfer to a Place of Deposit	Press releases may form a significant part of the public record of an organisation which may need to be retained

Public consultations	End of consultation	5 years	Review and consider transfer to a Place of Deposit	
Website	Creation	6 years	Review and consider transfer to a Place of Deposit	

Record Type	**Retention start**	**Retention period**	**Action at end of retention period**	**Notes**
11. Staff Records & Occupational Health Although pension information is routinely retained until 100th birthday by the NHS Pensions Agency employers must retain a portion of the staff record until the 75th birthday.				
Duty Roster	Close of financial year	6 years		Review and if no longer needed destroy
Exposure Monitoring information	Monitoring ceases	40 years/5 years from the date of the last entry made in it	Review and if no longer needed destroy	A) Where the record is representative of the personal exposures of identifiable employees, for at least 40 years or B) In any other case, for at least 5 years.
Occupational Health Reports	Staff member leaves	Keep until 75th birthday or 6 years after the staff member leaves whichever is sooner		Review and if no longer needed destroy
Occupational Health Report of Staff member under health surveillance	Staff member leaves	Keep until 75th birthday		Review and if no longer needed destroy
Occupational Health Report of Staff member under health surveillance where they have been subject to radiation doses	Staff member leaves	50 years from the date of the last entry or until 75th birthday, whichever is longer		Review and if no longer needed destroy

Staff Record	Staff member leaves	Keep until 75th birthday (see Notes)	Create Staff Record Summary then review or destroy the main file	This includes (but is not limited to) evidence of right to work, security checks and recruitment documentation for the successful candidate including job adverts and application forms. May be destroyed 6 years after the staff member leaves or the 75th birthday, whichever is sooner, if a summary has been made.
Staff Record Summary	6 years after the staff member leaves	75th Birthday	Place of Deposit should be offered for continued retention or Destroy	Please see the good practice box Staff Record Summary used by an organisation.
Timesheets (original record)	Creation	2 years	Review and if no longer needed destroy	