Policy:

IMST008 Records Management

Executive Director Lead	Executive Director of Finance
Policy Owner	Information Governance Manager
Policy Author	Data Protection Officer, Clinical Risk and Patient Safety Advisor

Document Type	Policy
Document Version Number	Version 3.3
Date of Approval By PGG	05/2024
Date of Ratification	July 2024
Ratified By	ARC
Date of Issue	May 2024
Date for Review	04/2027

Summary of policy

This policy governs the creation and use of records within the Trust.

Target audience	All people working on Trust business

Keywords	Records Management, Care Records, Corporate Records, Retention, Disposal

Storage & Version Control

Version 3.3 of this policy is stored and available through the SHSC intranet/internet. This version of the policy supersedes the previous version (V3.2 11/2023). Any copies of the previous policy held separately should be destroyed and replaced with this version.

Version Control and Amendment Log (Example)

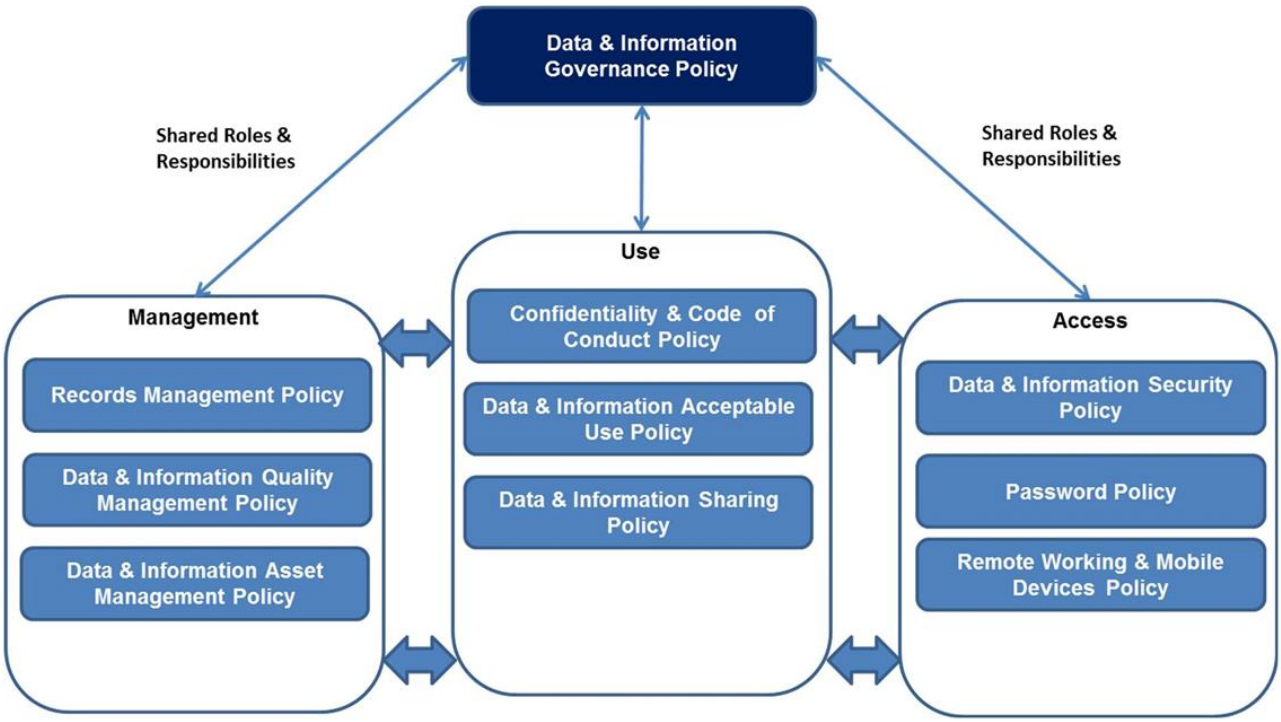
Version No.	Type of Change	Date	Description of change(s)
1	Policy ratified by EDG	January 2009	
2	Revisions submitted to Care Records Group	January 2011	
3	Revisions requested by Information Governance Steering Group	January 2011	
4	Revisions requested by Performance Information Group	January 2011	
5.9	Revised policy ratified by EDG	February 2013	
6.0	Updated version submitted to Information Governance Steering Group	March 2016	Updated for electronic records – detailed guidance for manual records formats removed
6.1	Updated for organisational changes and reformatted	October/ November 2016	Organisational changes – governance groups and responsibilities, addition of retention & disposal appendix to replace separate Retention, Disposal and Destruction of Care Records Policy; addition of reference to Accessible Information Standard and Appendix on Copy Letters to Service Users
7.0	Ratification / issue	November 2016	Ratification, finalisation and issue
7.1	Revisions requested by DIGB	August 2017	Addition of guidance for recording of gender change on Insight and access to records held by Sheffield Archives
7.2	Further revisions to update and streamline the policy	February 2018	Included in wider revision of Information Governance policies
3	Re-numbered	August 2018	Re-numbered version
3.1	Revision	Apr – Oct 2019	Updates for legislative and monitoring changes and contact details.
3.2	Revision	Aug 22 – Nov 23	Update for organisational change. Simplification of specified roles. Addition of FOI and SARs sections. Removal of the Appendix on Care Records Standards

3.3	Revision	April 2024	Improved records keeping guidance added following CQC recommendations

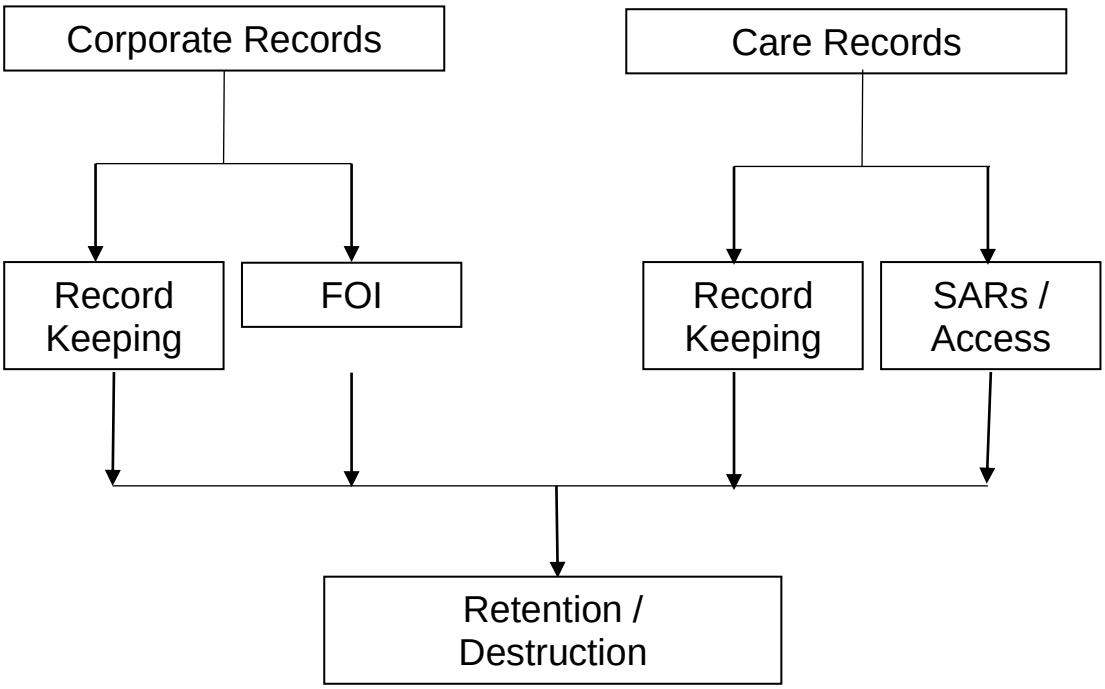
Contents

Flowchart

The Data & Information Governance Policy provides the overarching shared roles and responsibilities needed to satisfy complete trust Data, Information and System ownership and management.



Records management covers both corpprate and care records.



1 Introduction

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

Records Management, through the proper control of the content, maintenance and volume of records, reduces vulnerability to legal challenge or financial loss, supports compliance with legislation and standards, improves control of valuable information resources and promotes best value in terms of human and space resources.

Within the overall context of Records Management, care records have a fundamental role in the provision of safe, effective, high quality, evidence-based treatment and care to service users. Accurate and comprehensive recording of information is essential for service user care and continuity of communication between practitioners.

There are legal obligations that apply to the management of records and the Trust will take action as necessary to comply with these obligations. In particular, all NHS records are Public Records under the Public Records Acts. This Trust, in common with all NHS organisations, has a duty under the Public Records Act 1958 to make arrangements for the safe keeping and eventual disposal of all types of its records. In addition it needs robust records management procedures to meet its obligations, particularly under Data Protection legislation, the Access to Health Records Act 1990, the Common Law Duty of Confidentiality, Article 8 of the Human Rights Act 1998 and the Freedom of Information Act 2000. Further information about legal obligations is provided in section 11 of this policy.

This policy aligns to the NHSx Records Management Code of Practice (2021) for best practice and statutory obligations.

2 Scope

The scope of this document is to outline the Trust's policy for Records Management for all data, information and system management and protection.

This policy applies to all staff and services within the Sheffield Health & Social Care FT (SHSC), including private contractors, volunteers and temporary staff and to those organisations where we provide commissioned services.

Shared governance and compliance areas for data and information include:

- NHS Digital & England Guidance
- Data Security & Protection Toolkit
- Cyber-Security Best Practices
- Information Technology Service Management
- General Data Protection Regulation
- Caldicott Principles
- Data & Information Quality Management
- ISO27001 Information Security Management Systems

The policy supports the Trusts needs to continually improve, protect and manage all digital, data and information assets according to legislation and best practice through a collaborative approach.

Systems
All manual and electronic information systems owned, operated or managed by the Trust, including networks and application systems, whether or not such systems are installed or used on Trust premises.

Other systems brought onto Trust premises including, but not limited to, those of contractors and third party suppliers, which are used for Trust business.

Users
All users of Trust information and/or systems including Trust employees and non-Trust employees who have been authorised to access and use such information and/or systems.

Data & Information
All information collected or accessed in relation to any Trust activity whether by Trust employees or individuals and organisations under a contractual relationship with the Trust.

All information stored on facilities owned or managed by the Trust or on behalf of the Trust.

All such data and information belongs to the Trust unless proven otherwise.

3 Purpose

This policy defines a structure for the Trust to ensure adequate records are created and that they are managed in a systematic and planned way from the moment they are created through to their ultimate disposal. It ensures that the Trust can control both the quality and the quantity of the information it generates, that it can maintain the information in a manner that effectively serves its needs, the needs of its service users and the needs of others to whom it is accountable or are affected by or have an interest in its actions and decisions; and that it can dispose of the information efficiently when it is no longer required.

Records Management is a key component of the Information Governance framework for the NHS. The Trust will ensure that the way it manages its records is fully integrated with other Information Governance work areas.

This policy is intended to be complementary to the good record keeping practice set out in various professional codes of conduct.

4 Definitions

Records
Defined as recorded information, in any form, created or received and maintained by the Trust in the course of its business, providing evidence of its functions, activities and transactions.

Records Management
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-

- Record creation;
- Record keeping;
- Record maintenance (including tracking of record movements);
- Access and disclosure;
- Closure and transfer;
- Appraisal;
- Archiving; and
- Disposal.

Record Lifecycle
Describes the life of a record from its creation or 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 preservation in an archive.

Data & Information Governance
Overarching policy of requirements for handling data, information and systems in a secure and confidential manner according to the best legal, ethical and quality standards detailed in the Data & Information Governance Policy.

5 Detail of the policy

This policy regulates the creation, use, storage and destruction of care records and corporate records within the Trust.

6 Duties

Combines traditional Information Asset (IAO / IAA), data governance, data quality and (ITSM) system management roles and responsibilities into a single accountable shared Business Information Management framework.

Role		Responsibility	Description
Chief Digital Information Officer	CDIO	Chief Digital Information Officer	Responsible for the Information Technology that supports the overarching strategies of the Trust.
Chief Clinical Information Officer	CCIO	CCIO	Providing a vital voice for clinical strategy, allowing new IT, Data & Information products to help improve the provision of healthcare.
Senior Information Risk Owner	SIRO	Director Finance	Owns the Trusts information risk policy and risk assessment process.
Caldicott Guardian	CG	Director Medical	Responsible for protecting the confidentiality of patient and service user information and enabling the appropriate level of information sharing.
Information Governance Manager	IG Mgr	IG Manager	Leads information governance within the Trust

Data Protection Officer	DPO	DPO	Supporting Trust - wide Data & Information governance in accordance to GDPR, NHS Digital & England and Data Security & Protection Toolkit.
Cyber Security Officer	CSO	Assistant Deputy Directors, IMST	Supporting the Trust to continuously assess, implement and manage Trust wide cyber-security, and removing identified vulnerabilities with support from all technical and business managers and users.
Information Asset Owners	IAO	Directorate	Senior representatives of the directorates closely aligned to major stores of organisational data, information and systems.
Information Asset Managers	IAM	System/Service Managers	Primary administrative and management responsibilities for segments of data primarily associated with their functional area.

Each Data and Information role has clear responsibilities for data, information and system management within their respective service domains and role accountability, supported by natural hierarchy escalation and incident management.

All staff who use Trust information systems (including manual systems as well as electronic ones) plus other authorised users of systems are required to adhere to this policy.

7 Procedure

All care and corporate records have a fundamental role to play in the provision of safe, effective, high quality, evidence-based clinical care and effective corporate decision making and personnel management.

Information contained within all records must be recorded accurately, be current, contemporaneous, comprehensive and concise, support effective future action, evidence and legal document requirements.

Staff must ensure that, where manual records remain in existence, they have the complete record, both manual and electronic, available to them, when it is needed.

Whether manual or electronic, the responsibility for the contents and care of records lies with all Trust staff that handle, write and maintain them.

Set out below are the policy aims for effective management of SHSC's records in order to ensure that:

- Records are available when needed
- Records can be accessed (located and displayed) when needed
- Records can be interpreted
- Records can be trusted
- Records can be maintained and accessed over time despite any changes in format
- Records are secure from unauthorised access, alteration or destruction

- Records are retained and disposed of appropriately

NHS England guidance states “Emails and text messages in the health and care setting are a professional communication. Any message together with any response received with the time and dates should be noted on the patient/service user record.” Relevant information from e-mail exchanges should be added to the care record but do not add routine, transactional information such as copies of e-mail delivery receipts which do not contribute to the care of the service user

It is a fundamental requirement that all of the Trust’s 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 the Trust’s functions.

In cases of doubt about retention periods or about retention and disposal arrangements please contact the appropriate Records Management Lead for guidance. (See section 14 for contact details)

Where the Trust holds joint Health and Social Care and Corporate records there may be cases where a record is covered by different retention periods - these records should be retained for the longest period for that type of record.

The Trust will follow the minimum retention periods set out in the NHS **Records Management Code of Practice** which provides detailed guidance on minimum retention periods for different categories of record.

7.1 Standards of Record Keeping

All SHSC staff are required to follow these guidelines:

- Complete records at the time or as soon as possible after an event, recording reason for delay and actual time of the event being reported if a note is written sometime after the event.
- It is expected SHSC practice that the time of the clinical interaction/event is documented in the clinical record regardless of the time of entry writing. (The electronic patient record will automatically record the time of writing – but not the time of the incident/event/interaction).
- Taking the above into account, all records MUST be made at the end of a clinical shift/day for patients seen/incidents and events.
- In the highly unusual event that records cannot be made at the end of a clinical shift, this must be reported to the professional in charge/line manager for the team and a verbal account given of any patients seen. Handwritten notes must be made at the end of the shift/day and transcribed into the clinical record as soon as possible (usually the next working day).
- Where a record refers to multiple events this must be made clear in the record.
- All conversations with carers, relatives or significant others must be recorded in the clinical records within the same day as contact or by exception in agreement with the line manager.
- All conversations with associated staff, external parties or professionals must be recorded in the clinical records within the same day as contact or by exception with the line manager.
- It is not Trust policy to restrict access to specific notes or documents on the EPR beyond the general access controls afforded by the system so notes or documents will not be individually locked or password-protected. If a matter

arises that requires information to be withheld from the wider clinical team, this should be discussed with the service manager and the Chief Clinical Information Officer/Caldicott Guardian.

- Complete records accurately and without any falsification, taking immediate and appropriate action if you become aware that someone has not kept to these requirements.
- Digital notes written outside the EPR and then imported into the system must be traceable to the person who provided the care that is being documented.
- Records are disclosable in a court of law and to service users and families and as such should be written using a language and format suitable for this.
- Record keeping can be delegated to non-registered practitioners such as support workers and nursing students so that they can document their care. As with any delegated activity, the practitioner needs to ensure that the non-registered practitioner or student is competent to undertake the activity and that it is in the patient's best interests for record keeping to be delegated.
- Supervision and a countersignature are required until the non-registered practitioner or student is deemed competent at keeping records. Competency should be assessed at team level. Area managers should ensure they have a system in place to sign off competency for record keeping in non-registered staff.
- You should use your judgement to decide what is relevant and what should be recorded however, all entries should be complete and adequate for the purpose.
- Record facts clearly and where the facts lead to a deduction or opinion make it clear that the statement is an opinion.
- Beware of writing judgemental statements, where you are not in a position to judge.
- All entries must be written in a clear and unambiguous style.
- Records should not include jargon, meaningless phrases (e.g. comfortable night), irrelevant speculation or offensive subjective statements. All statements must be factual.

Handwritten/Paper notes

- All records must be signed, timed and dated if handwritten.
- Records should be legible when photocopied or scanned.
- In the rare case of needing to alter a record, the original entry must remain visible (draw a single line through the record and sign as the practitioner altering). The new entry must be signed, timed and dated.
- All handwritten notes should be transferred to the electronic patient record and original paper notes disposed of in a confidential waste bin.
- All documents received should be scanned onto the electronic patient record and original copies disposed of in a confidential waste bin.

What makes a good record?

Right Login - All entries must be made under your own log in.

Right Record - You must make sure you are in the correct patients record before you start adding your entry.

Right Team - Ensure you are making your entry against the right team.

Right Place:

- Check that all clinical records are being made on the correct form, document or template.
- All records relating to patient care including waiting list, management of patient flow and allocation must be held within the EPR. Any records held outside the EPR for such purposes must be recorded in the Directorate Risk Register

Right Time:

- Ensure record entries are made in the correct chronological order where possible.
- Every effort must be made to make sure all entries are recorded within a reasonable time frame of the event and at least by the end of a clinical shift/day for all patients seen, incidents and events.
- Late entries should make clear the reason for delay and the length of delay.
- In the very rare event of it not been possible to make a timely record you should provide a verbal handover of key clinical information to the nurse in charge or clinical lead in your area.

Right detail included:

- Keep a clear record of staff members involved including name, job title and role in full.
- Make sure actions taken & reasoning is clearly recorded and is relevant to the entry.
- Ensure key information such as, allergy status is recorded.

Right wording used:

- Avoid use of abbreviations, or where used write in full first.
- Ensure enough information is recorded to make the entry clear and to the point.
- All entries must be appropriate, clear, factual, relevant and where possible, reflect your patients views who should be able to understand what the record says.
- Records should be attributable to yourself, free from unnecessary jargon & speculation.

Right communication used:

- Ensure next of kin and preferred language are recorded.
- Check demographics including contact numbers on a regular basis.
- Record alternative point of contact such as nominated carer or relative.
- Ensure you understand respect and use your patients' preferred forms of communication.

Care and Treatment Planning

- Ensure your patient has a current care and treatment plan recorded on the Collaborative Care Plan or approved local template.
- Make sure that care and treatment plans are routinely produced collaboratively with your patient and that their views, opinions and preferences are clear to the reader.
- Ensure your patient is offered a copy of the care and treatment plan in a format that they can easily understand.
- Refusal to accept a care and treatment plan must be recorded in the collaborative care plan, local template or notes.
- Avoid jargon and abbreviations, your audience is your patient

Risk Management

- Ensure your patient has an up-to-date risk assessment.
- Ensure your risk assessment is personalised and co-produced with your patient, their carer and the wider MDT where appropriate.
- Clinical risk assessments should include the patient's own narrative about their own risks.
- The clinical risk assessment should:
  - Include meaningful activities to manage risk.
  - Adopt a positive risk management approach.
  - Follow a strengths based approach which is realistic and achievable.
  - Not contain risks rating scales such as "Low, Medium or High" and instead refer to predisposing, precipitating, perpetuating and protective factors as part of your risk planning.

Adherence to the above principles contributes to the maintenance of "***GREAT***" clinical records.
Good quality. ***R***elevant and Individualised. ***E***vidence patients voice. ***A***ccurate and complete. ***T***imely

7.2 Care Records

Care records are a means of communication between practitioners and between practitioners and the service users. They are sometimes called in evidence before a court during legal proceedings.

Care records should contain the relevant findings in the health and care of the person receiving treatment or care and should provide clear evidence of the care planned, the decisions made, the care delivered and the information shared.

7.3 Corporate Records

Corporate records are a means of logging, communicating and managing corporate trust action and supporting services for all staff

Corporate information refers to information generated and received by a service other than clinical / care (i.e. service user) information. The term describes the records generated by an organisation's business activities, and therefore will include records from the following (and other) areas of the organisation:

- Digital Directorate
- People Directorate & Finance
- Corporate Governance
- Training

7.4 Freedom of Information

As a Public Authority, the Trust is subject to the requirements of the Freedom of Information Act 2000 (FOI). This makes information held by Public Authorities accessible to the public by providing a 'right to know' rather than restricting access on a 'need to know' basis.

Under the Act, the Trust must maintain a Publication Scheme which details all of the information which it publishes proactively, such as such as policies and procedures, minutes of meetings, annual reports and financial information. The Publication Scheme is available on the Trust's external website.

The Act also gives people the right to make Freedom of Information requests for information held by the Trust.

FOI requests can me made by anyone and can be submitted anywhere within the Trust so all staff need to know how to recognise a request and how do deal with them.

Requests may be submitted to:

shsc@infreemation.co.uk

although they may also be submitted elsewhere in the Trust. Infreemation is the system used by the Trust to administer FOI requests.

FOI requests must be made in writing, must include the applicant's real name and give an address for correspondence (e-mail addresses are sufficient).

Routine requests for information which can be answered immediately need not be treated as formal FOI requests but requests involving more work to identify, locate and retrieve the requested information, or requests that specifically state that they are made under the Freedom of Information Act, should be treated as formal FOI requests and notified to the Information Governance Team. The Information Governance Team will log formal requests and manage their processing.

Requests must be processed within 20 working day, starting from the time the request is received. Clarification may be sought if it is not clear what information is being requested.

Information need not be created in order to answer a request.

There are certain exemptions which may apply to requests – the most common are the exemption for personal information, requests which would take more than a specified time limit to comply with, information supplied in confidence and information intended for future publication.

Person-identifiable information such as care records, is exempt from disclosure under FOI, although it may be accessible to data subjects and their representatives as a Subject Access Request under the Data Protection Act 2018/UK GDPR. Where data subjects attempt to access their own information under FOI this will be treated as a Subject Access Request under UK GDPR. FOI is more relevant to non-personal information held by the Trust such as Corporate Records.

The Information Governance Team will decide whether any exemptions are applicable to a request, and will apply a public interest test where this is required.

FOI requests are supplied free of charge and are processed 'purpose-blind' – the applicant's reason for making a request is irrelevant, except in the very rare occasions that requests are deemed to be vexatious (again, the Information Governance Team will decide whether this applies).

Information about the environment is covered by the Environmental Information Regulations (EIR) rather than the Freedom of Information Act – these are similar but with some differences. The Information Governance Team will determine whether EIR is relevant so staff receiving a request which may be covered by the EIR should notify them as with ordinary FOI requests.

On receipt of a request, either directly or forwarded from another department, the Information Governance Team will:

- log receipt of the request
- verify that it is a valid request (or notify the applicant if it is not)
- acknowledge receipt of the request
- seek clarification if necessary
- identify whether the requested information is held, liaising with other departments as necessary
- assess whether any exemptions apply
- notify the appropriate team(s) of the information required and the necessary timescales
- track the processing of the request and issue reminders if necessary

- compose and send a response to the applicant

Where the specific information requested is not held but similar information which may be of interest to the applicant is held they will be notified of this fact.

Where the Trust does not hold the information requested but it is believed that another Public Authority may hold it, the request will not be transferred to that organisation but the applicant will be told that they may wish to contact them.

Numbers of requests received and processed will be reported to Trust senior management to provide assurance that legal requirements are being met.

Processing of FOI requests will be expedited by good record keeping – ensuring that the Trust knows what records it holds and destroying them when no longer needed in accordance with the specified retention periods (although records must not be destroyed simply to avoid disclosing them). Records should be composed in the expectation that they may be disclosed and so their content must be appropriate and professional.

7.5 Subject Access Requests

Where records contain personal information about identifiable, living individuals, the data subjects have the right to access or obtain copies of the information by making a Subject Access Request (SAR). Requests will be overseen by the Information Governance Team but all staff must be able to identify and deal with requests.

SARs can be verbal as well as written and can be made anywhere within the Trust so it is important that all staff are able to recognise them and make sure they are processed. Forms are provided on the Trust external website:

https://www.shsc.nhs.uk/contact-us/accessing-your-health-records

Applicants are not obliged to use these forms but they will help to expedite requests. They include details of the proof of identity required to verify requests.

Third-parties may make a Subject Access Request on behalf of a data subject with the appropriate consent or authority.

We have one month to respond to SARs (except where they are judged to be complex, in which case the time limit can be extended by a further two months). The Information Governance Team will advise on when requests can be considered complex.

If staff receive a Subject Access Request they should forward it to the Information Governance Team without delay. Requests may also be made directly to the Information Governance team by data subjects and may also be submitted via the Infreemation online system.

Once a formal request has been submitted, the Information Governance Team will identify whether the requested records are held and if so, extract the records and perform checks for any third party information which may need to be redacted before release.

Medical records have to be reviewed for any information which would be likely to cause serious harm to the data subject or another person if they were released – this decision has to be made by an appropriate health professional so the Information Governance Team will contact clinicians to request these checks to be completed. If any such information is identified, the health professional will notify the Information Governance Team who will make the necessary redaction, unless it is necessary to withhold the entire record.

The Information Governance Team will monitor progress of requests against the required timescales and will issue responses when complete, using the applicant's preferred medium where possible - records sent electronically will be sent securely but if the applicant requests paper copies these will be sent via special delivery or offered for collection from a Trust base on production of proof of identity.

As with Freedom of Information requests, numbers of Subject Access Requests received and processed will be reported to Trust senior management.

If a Subject Access Request is made for CCTV/Surveillance Camera footage, the Information Governance Team will liaise with the identified owner of the relevant system who will be responsible for extracting the relevant footage and ensuring that no third-party information is included without consent.

The Information Governance Team will also co-ordinate requests from other external sources such as other NHS Trusts, social services and the police

7.6 Training

All staff and others working on Trust business are made aware of their responsibilities for record keeping and record management through generic and specific training programmes and guidance. Further information on training and awareness is contained in section 8 below.

7.7 Accessible Information Standard

From 31 July 2016 Health and Social Care organisations are required to meet the Accessible Information Standard which is a legally enforceable standard to support service users and carers with a disability, impairment or sensory loss.

The standard has been introduced to make sure that disabled people have access to understandable information and relevant communication support.

The standard requires organisations to:

- IDENTIFY that someone has a NEED linked to a disability
- RECORD information about the NEED
- MEET this NEED
- SHARE information about this NEED

The EPR has the facility to record NEEDS so that information that a person has a NEED recorded is flagged when the system is accessed.

Further information about the standard is provided in the Accessible Information and Communication Policy.

7.8 Reporting Incidents and Weaknesses

An Information Incident is an event that could compromise the confidentiality of information (if it is lost or could be viewed by or given to unauthorised persons), the integrity of the data (if it could be inaccurate or content could have been changed) or the availability of the information (access).

Examples of information incidents are:

- Potential and suspected disclosure of NHS information to unauthorised individuals.
- Loss or theft (attempted or actual) of paper records, data or IT equipment on which data is stored.
- Disruption to systems and business processes.
- Attempts to gain unauthorised access to computer systems, e.g. hacking.
- Records altered or deleted without authorisation by the data "owner".
- Virus or other malicious malware attacks (suspected or actual).
- "Blagging" offence where information is obtained by deception.
- Breaches of physical security e.g. forcing of doors or windows into secure rooms or filing cabinets containing sensitive information left unlocked in an accessible area.
- Leaving a desktop or laptop unattended when logged-in to a user account without locking the screen to stop others accessing information.
- Human error such as emailing data by mistake.
- Covert or unauthorised recording of meetings and presentations.
- Damage or loss of information and information processing equipment due to theft, fires, floods, failure of equipment or power surges.
- Deliberate leaking of information.
- Insider fraud.[1]
- Smartcard or application misuse.
- Smartcard theft.
- Non-compliance of local or national RA policy.
- Any unauthorised access of NHS applications.
- Any unauthorised alteration of patient data.

The Trust handles considerable amounts of patient data, much of which is sensitive. An information incident involving sensitive data, especially patient confidential information, is considered to be a data/information breach and must be reported.

All information management and technology security incidents and weaknesses must be reported via Trust incident reporting procedures (see Trust Incident Management Policy and Procedure).

Incidents that present an immediate risk to the Trust should be escalated through local supervisor & manager, IT Service Desk & Data Protection Officer.

7.9 SIRO & Data & Digital Assurance Group Reporting (DAG)

The Information Governance Manager will keep SIRO & DAG informed of the information incidents status by means of regular reports and immediate alerts where an immediate risk is identified.

[1] Where any incidents involving suspected fraud are identified, the Trust's Counter Fraud, Bribery and Corruption Policy should be followed and advice sought from the Local Counter Fraud Specialist (christaylor2@nhs.net).

8 Development, Consultation and Approval

Previous versions of the policy were developed under the Care Records Group, Information Governance Steering Group and Performance Information Group.

The review leading to this version of the policy was commissioned by the Information Governance Steering Group in March 2016 with further amendments under the authority of the Data & Information Governance Board in October 2016.

It incorporates recommendations from the Information Governance Toolkit Audit for 2015/16.

The policy was revised to include guidance for recording of gender change on Insight and access to records held by Sheffield Archives in February 2017.

This policy was reviewed as part of a major review of Information Governance policies in 2018 to meet the requirements of legislative change (introduction of the General Data Protection Regulation (GDPR) and Data Protection Act 2018) and the migration from the Information Governance Toolkit to the Data Security & Protection Toolkit which takes account of the National Data Guardian's data security standards.

The policies were approved by the Data & Information Governance Board in May 2018.

This policy was updated in October 2018 to update references and contact details for submission to the November 2019 Data & Information Governance Board.

This policy was reviewed in August 2022 following discussion within IMST and in preparation for submission to the September 2022 Data & Information Governance Group meeting. Further minor updates for organisational change and addition of the FOI and SARs sections in summer 2023, prior to submission to the Digital Assurance Group in September 2023. It was approved by the DAG.

The policy was submitted to EMT in November 2023 resulting in the removal of 'Appendix C – Care Records Standards' in anticipation of a new, separate policy on record keeping.

Additional guidance on record keeping was added in April 2024 instead of developing a separate policy.

9 Audit, Monitoring and Review

This section should describe how the implementation and impact of the policy will be monitored and audited. It should include timescales and frequency of audits.

If the policy is required to meet a particular standard, it must say how and when compliance with the standard will be audited.

Monitoring Compliance Template						
Minimum Requirement	Process for Monitoring	Responsible Individual/ group/committee	Frequency of Monitoring	Review of Results process (e.g. who does this?)	Responsible Individual/group/ committee for action plan development	Responsible Individual/group/ committee for action plan monitoring and implementation
Duties	Local induction, PDR, Supervision	Line Managers	At least annually	Directorates	DAG	DAG
Legal obligations that apply to records	Supervision PDR	Line Managers	Annual	Directorates	DAG	DAG
How a new Record is created	Clinical Records Audit	Directorates	Annual	Clinical Audit	DAG	DAG
How health records are tracked when in current use	Electronic records stored centrally and subject to audit trail	DAG	Ongoing	Directorates	DAG	DAG
How health records are retrieved from storage	Supervision PDR	Line Manager	Annual	DAG	DAG	DAG

Process for retention, disposal and destruction of records	Retention & Disposal Schedule	DAG	Annual	DAG	DAG	DAG
Basic Records keeping standards which must be used by all staff	Clinical Records Audit	Directorates	Annual	Clinical Audit	QAC	QAC
Process for making sure a contemporaneous record of care is completed	Clinical Records Audit	DAG	Annual	Clinical Audit	QAC	QAC
How the organisation trains staff in line with the TNA	Supervision PDR Training records	Directorates Training Dept.	Annual	DAG	DAG	DAG

The Trust will ensure that an audit of records management practices will be regularly included in the Internal Audit work programme and that reports and recommendations for corrective action are fed back to the Audit and Assurance Committee.

The Digital Assurance Group (DAG) will ensure arrangements are established to test compliance of records management procedures and practices with the provisions of this policy and with associated standards, including NHS Litigation Authority Risk Management Standards and Data Security & Protection Toolkit Requirements, to identify areas requiring attention in future work programmes.

With regard to care records, record keeping standards for all professional groups will be periodically audited through the clinical audit process.

All audits involving physical records must be undertaken at the location where the records are held. Records must not be taken off the premises, including photocopies and print-outs of scanned documents etc.

The Digital Assurance Group will oversee and sign off the content of annual work programmes to support implementation of the policy, and will monitor actual progress with the programmes.

Issues and progress on records management covering all records will be fed back to the Digital Assurance Group, who in turn will feedback to the Trust Board, through providing the necessary assurances to the Quality Assurance Committee.

This policy will be reviewed three years after ratification, or sooner if major changes occur in legislation, guidance or in other policies which have an impact on Records Management.

10 Implementation Plan

Action / Task	Responsible Person	Deadline	Progress update
Dissemination Post on Trust intranet. Ensure all staff in directorate teams are aware of this policy and their responsibilities under it.	 RM leads Heads of directorates	 Within 7 days of ratification	
Review and update organisational arrangements. Review and update Lead roles for Records Management.	Board level RM leads Board level RM leads	At each policy review	

11 Dissemination, Storage and Archiving (Control)

This section should describe how the new policy will be disseminated. It says where the policy will be made available and to whom. This will normally be that the policy is available on the Trust's intranet and available to all staff.

It makes it plain that any previous versions must be deleted and describes the archiving and storage arrangements for the current and previous versions of the policy.

It says who is responsible for archiving and version control, and what they should do.

Version	Date added to intranet	Date added to internet	Date of inclusion in Connect	Any other promotion/ dissemination (include dates)
3.0	08/2018	08/2018		
3.1	11/2019	11/2019		
3.3	07/2024	07/2024		

12 Training and Other Resource Implications

Information Governance training is mandatory for all staff on induction and on a yearly basis.

The Information Governance Team will work with the Training team and managers to ensure that appropriate additional training is available to support staff.

The Information Governance team will work the Senior Information Risk Owner, Information Asset Managers and other appropriate managers and teams to maintain continued awareness of confidentiality and security issues to both the organisation and staff through staff emails, newsletters, intranet etc.

Standards of Good Clinical Record Keeping training is mandatory for all staff on induction and on a three yearly refresher basis. The training is mandatory to all clinical staff who add/input service user/service specific information into the electronic patient record system.

This includes (but is not exhaustive of):

- AHP Staff
- Medical Staff
- Nursing Staff
- Healthcare/Auxiliary Staff
- Pharmacy Staff

The Quality Directorate Team will work with the Learning Development team and managers to ensure that appropriate additional training is available to support staff.

13 Links to Other Policies, Standards (Associated Documents)

Further information about Records Management requirements is contained in the NHS Records Management Code of Practice. This Code of Practice is a guide to the standards of practice in the management of records for those who work within or under contract to NHS organisations. It is based on current legal requirements and best professional practice.

It underpins this policy.

The Code of Practice is available alongside this policy on the Trust's Intranet.

Attention is drawn to the following legislation which has significant implications for Records Management:

<u>Data Protection Legislation</u>
A key driver for compliance with records management principles is the Data Protection Act 2018 which enacts the General Data Protection Regulation into UK law. These acts regulate the processing of personal data, held both manually and on computer. Personal data is data relating to a living individual that enable him/her to be identified from that data alone or from that data in conjunction with other available information.

Processing of personal data includes everything done with that information, for example, obtaining, holding, recording, using, disclosing and sharing it.

Access to Health Records Act 1990

This Act remains in force only in respect of the health records of deceased patients. It applies only to records created since 1 November 1991. This Act provides rights of access to the health records of deceased individuals for their personal representatives and others having a claim on the deceased's estate. In other circumstances, disclosure of health records relating to the deceased should satisfy common law duty of confidence requirements.

Freedom of Information Act 2000

Good records management is also a pre-requisite for compliance with the Freedom of Information Act 2000. See section 7.3 above.

Common Law Duty of Confidentiality

Common Law is not written out in one document like an Act of Parliament. It is a form of law based on previous court cases decided by judges; hence it is also referred to as case law. The general position is that if information is given in circumstances where it is expected that a duty of confidence applies, that information cannot normally be disclosed without the information provider's consent. In practice this means that all service user information, whether held on paper or electronically, or held in the memory of a practitioner, must not normally be disclosed without the consent of the service user. Three circumstances making disclosure of information lawful are:

- where the individual to whom the information relates has consented;
- where disclosure is in the public interest; and
- where there is a legal duty to do so, e.g. a court order.

All staff involved in the management of records must be aware of their responsibility for maintaining confidentiality of records. If in doubt seek help.

Human Rights Act 1998

The Act became part of UK law on 2 October 2000. Article 8 provides that each individual has a right to respect for his/her private life, and that right may only be interfered with in accordance with law and to the extent that it is necessary in a democratic society in the interests of national security, public safety, the economic well-being of the country, the prevention of disorder or crime, the protection of health or morals or the protection of the rights and freedoms of others. The European Court has held that the individual's private life protected by Article 8 includes his/her medical records and that respect for their confidentiality is a fundamental human right. It was held that the protection of patient confidentiality is vital both to an individual's own sense of protection of his/her private life and to the preservation of public confidence in the medical profession and health services in general.

Current understanding is that if Trusts comply with the provisions of the Common Law Duty of Confidentiality and Data Protection legislation they will meet the requirements of Article 8.

More information on the application of Data Protection legislation, the Access to Health Records Act, the Common Law Duty of Confidentiality, the Human Rights Act and the Freedom of Information Act and on the records management implications of

other legal and professional obligations can be found in NHS “Records Management Code of Practice”.

14 Contact Details

Title	*Name*	*Phone*	*Email*
Trust Records Management Lead for Care Records	TBA		
Trust Records Management Lead for Corporate / Business Records	Deborah Lawrenson, Director of Corporate Governance	2716767	deborah.lawrenson@shsc.nhs.uk
Board level Director for Records Management – Care Records	TBA		
Board level Director for Records Management - Corporate / Business Records	Salma Yasmeen, Chief Executive	2716716	salma.yasmeen@shsc.nhs.uk
Caldicott Guardian	Helen Crimlisk, Interim Medical Director	2716383	helen.crimlisk@shsc.nhs.uk
Mental Health Act Administrator	Mike Haywood	2718102	mike.haywood@shsc.nhs.uk
CDIO & Director of Digital	Chris Reynolds	2664960	chris.reynolds@shsc.nhs.uk
Clinical Risk and Patient Safety Advisor	Darren McCarthy	2663605	darren.mccarthy@shsc.nhs.uk
Information Governance Manager	Katie Hunter	0114 2716723	katie.hunter@shsc.nhs.uk
Trust Data Protection Officer	John Wolstenholme	3050749	john.wolstenholme@shsc.nhs.uk
Board level Lead for Freedom of Information	Phillip Easthope, Executive Director, Finance	2716716	phillip.easthope@shsc.nhs.uk
Trust Freedom of Information Lead	TBA		
Education, Training and Development Lead	Karen Dickinson	2263116	Karen.Dickinson@shsc.nhs.uk

Appendix A

Equality Impact Assessment Process and Record for Written Policies

Stage 1 – **Relevance** - Is the policy potentially relevant to equality i.e. will this policy potentially impact on staff, patients or the public? This should be considered as part of the Case of Need for new policies.

NO – No further action is required – please sign and date the following statement. **I confirm that this policy does not impact on staff, patients or the public.**	***I confirm that this policy does not impact on staff, patients or the public.*** Name/Date: J Wolstenholme, 05/04/2024	~~**YES,** Go to **Stage 2**~~

Stage 2 Policy Screening and Drafting Policy - Public authorities are legally required to have 'due regard' to eliminating discrimination, advancing equal opportunity and fostering good relations in relation to people who share certain 'protected characteristics' and those that do not. The following table should be used to consider this and inform changes to the policy (indicate yes/no/ don't know and note reasons). Please see the SHSC Guidance and Flow Chart.

Stage 3 – **Policy Revision** - Make amendments to the policy or identify any remedial action required and record any action planned in the policy implementation plan section

SCREENING RECORD	Does any aspect of this policy or potentially discriminate against this group?	Can equality of opportunity for this group be improved through this policy or changes to this policy?	Can this policy be amended so that it works to enhance relations between people in this group and people not in this group?
Age			
Disability			
Gender Reassignment			
Pregnancy and Maternity			

Race			
Religion or Belief			
Sex			
Sexual Orientation			
Marriage or Civil Partnership			

Please delete as appropriate: - Policy Amended / Action Identified (see Implementation Plan) / no changes made.

Impact Assessment Completed by:
Name /Date

Appendix B

Review/New Policy Checklist

This checklist to be used as part of the development or review of a policy and presented to the Policy Governance Group (PGG) with the revised policy.

		Tick to confirm
	Engagement	
1.	Is the Executive Lead sighted on the development/review of the policy?	✓
2.	Is the local Policy Champion member sighted on the development/review of the policy?	✓
	Development and Consultation	
3.	If the policy is a new policy, has the development of the policy been approved through the Case for Need approval process?	N/A
4.	Is there evidence of consultation with all relevant services, partners and other relevant bodies?	✓
5.	Has the policy been discussed and agreed by the local governance groups?	✓
6.	Have any relevant recommendations from Internal Audit or other relevant bodies been taken into account in preparing the policy?	✓
	Template Compliance	
7.	Has the version control/storage section been updated?	✓
8.	Is the policy title clear and unambiguous?	✓
9.	Is the policy in Arial font 12?	✓
10.	Have page numbers been inserted?	✓
11.	Has the policy been quality checked for spelling errors, links, accuracy?	✓
	Policy Content	
12.	Is the purpose of the policy clear?	✓
13.	Does the policy comply with requirements of the CQC or other relevant bodies? (where appropriate)	✓
14.	Does the policy reflect changes as a result of lessons identified from incidents, complaints, near misses, etc.?	✓
15.	Where appropriate, does the policy contain a list of definitions of terms used?	✓
16.	Does the policy include any references to other associated policies and key documents?	✓
17.	Has the EIA Form been completed (Appendix 1)?	✓
	Dissemination, Implementation, Review and Audit Compliance	
18.	Does the dissemination plan identify how the policy will be implemented?	✓
19.	Does the dissemination plan include the necessary training/support to ensure compliance?	✓
20.	Is there a plan to i. review ii. audit compliance with the document?	✓
21.	Is the review date identified, and is it appropriate and justifiable?	✓

Appendix C – Procedure for sending Manual Care Records out of Sheffield Health & Social Care NHS Foundation Trust

This procedure is to ensure that Care Records that are sent out of the Trust are done so in a safe and secure manner.

This procedure describes how the notes should be sent and by whom. This procedure does not cover who has the right to request access to the care records held by Sheffield Health and Social Care NHS Foundation Trust.

In most cases for anyone other than the service user to have copies of the notes authorisation must be given by the service user; however, authorisation is not always required when a Health or Social Care Professional who is currently looking after the service user makes the request.

Requests by Health Professionals not belonging to the Sheffield Health & Social Care NHS Trust should be made to the Information Governance Team.

Where the records are stored on the EPR, the Information Governance Team will then locate the appropriate records, seek authorisation from the appropriate professional and dispatch the approved records. For services using SystmOne, the Information Governance Team will liaise with the service to extract and review the records.

For requests that are not processed by the Information Governance Team the following procedure must be followed.

The request must state the records required and, except in the case of Subject Access Requests, the reasons the records are needed. Authorisation to send the records must by sought from the appropriate Health Professional.

Where possible, records should be provided in electronic format on media encrypted to national standards or via an approved file sharing service.

If records are to be sent via e-mail the e-mail must be encrypted – either between addresses which both belong to approved public sector domains (such as NHSmail) or using the SHSC encryption facility – see the Data & Information Sharing Policy for further details. Ordinary SHSC e-mail addresses are not sufficient without the message being specifically encrypted.

If paper copies are to be provided these must be sent by Special Delivery (signed for).

Appendix D – Retention, Disposal & Destruction of Records

1. Retention Periods

The Trust will adhere to the retention periods specified within the NHS Records Management Code of Practice (available via the SHSC Intranet).

This lists minimum recommended retention periods for various types of records including care records and corporate records.

Where records are held by the Trust for both Health and Social Care purposes and the retention periods for Health records differ from those for Social Care records, the Trust will adhere to the longer of the relevant retention periods.

Since the introduction of the Care Records Mandate, all care records should be electronic but where physical records (including paper and microfilm/microfiche) remain they will be governed by the same retention periods.

Where records have passed their minimum retention period they will be considered for archiving or disposal but records which may be relevant to any ongoing national inquiry must not be destroyed.

Requests to destroy records before they have reached their minimum retention period must be submitted to the Digital Assurance Group.

2. Specific Record Types

The major retention periods for records used within the Trust are as follows:

- For mental health records the current retention period is 20 years after the date of last contact between the service user and any heath/care professional employed by the mental health provider, or 10 years after the death of the service user if sooner.
- Research datasets – No longer than 20 years
- Board Meetings and major committees – up to 20 years
- DPIAs – 6 years
- Serious incidents – 20 years
- Risk registers – 6 years
- Staff records – until 75th birthday
- Disciplinary records – 6 years
- Smoking Cessation – 2 years from the end of the 12-week quit period
- Final Annual Accounts Reports – up to 20 years
- Financial transactions – 6 years
- Invoices – 6 years
- Salary information – 10 years

Other periods may be relevant depending on the specific type of record so in cases of doubt the guidance document must be consulted before destroying any care records. Where the appropriate retention period can still not be identified the matter should be referred to the Data Protection Officer.

Records held on SystmOne will follow national procedures in relation to retention and disposal. Retention and disposal of electronic records held on the EPR will be subject to the following process:

The minimum retention period should be calculated from the beginning of the year following the date of the last contact with the service user or the year in which the service user died.

The dates used in calculating the minimum retention period will be the date of death as recorded on the EPR or Archive Viewer for deceased people, or the latest of the last recorded activity, the last date of discharge from an inpatient or residential setting, or the last recorded note or document recorded for service users with no date of death (in the case of notes or documents the date used will be the date the note or document refers to, not the date it was made or scanned).

For client records transferred from an earlier system or other clients with no activity or notes recorded on the system and no date of death, the minimum retention period will be calculated from the date the client record was created.

Once records held on the EPR have reached their minimum retention period they will be removed from the system unless they are still in use. Such records will initially be moved to a secure archive storage area and may be deleted at a later date, subject to the approval of the Digital Assurance Group.

3. Physical Care Records

Where physical care records still exist they should be scanned onto the appropriate electronic patient information system which will hold the definitive care record. Once paper records have been scanned and the electronic copy verified, the electronic record becomes the definitive record and the original physical documents may be securely destroyed before the minimum retention period has been reached.

If physical care records are the only copy of the care record and they are not to be scanned then they must be retained for the appropriate retention period and destroyed securely when no longer needed.

4. Documentation of Archived/Destroyed Records

When care records of any format are archived or destroyed a record must be kept listing:

- the records destroyed, including destruction dates
- the name and designation of the senior manager authorising the destruction

- evidence of destruction e.g. a certificate of destruction from an external contractor, or details of method and place of destruction together with name and designation of Trust staff carrying out the destruction

5. Transfer of Records to Archives

The Trust has previously transferred a selection of service user records considered to be of archival value to the Sheffield Archives as the Approved Place of Deposit.

The Trust retains control of who can access those records already transferred to the archives. Requests for access to detailed records will not normally be granted until 100 years after the date of the record. In the case of requests for genealogical purposes the Trust will normally agree to confirm the dates of treatment and provide a copy of a photograph of the service user to family members if one is held.

Other requests for access to records held by the archives will be considered on their merits. The Caldicott Guardian will be the final arbiter for these requests.

At present there are no arrangements for the transfer of further electronic care records to the archives.

See Appendix H for further details.

6. Corporate/Organisational Records

Retention and disposal of organisational records will be managed subject to the same guidance as care records and under the overall authority of the Director of Corporate Governance.

7. Long-Term Storage

Where physical records are required to be kept for a period of time until their minimum retention period is reached but they are not required for current use, they may be placed in long-term storage.

Secure long-term storage may be provided on SHSC premises or in commercial off-site provision depending on the needs of the Trust.

The originating service remains responsible for records placed in long-term storage, including the documentation of records sent for storage, access to and retrieval of the records, and their final destruction.

The originating service must retain details of the contents of any records placed in long-term storage to allow for their recall if required and to arrange for their destruction when no longer needed.

It is the responsibility of the originating service to ensure that any records sent for long-term storage are contained in suitable boxes to the specification required by the storage facility (either internal SHSC storage or external commercial storage).

When placing records in long-term storage it is the responsibility of the originating service to ensure that the record boxes are accurately labelled with a summary of the contents, the contact details of the originating service and the date after which the records can be securely destroyed in line with national guidance on retention periods.

If the originating service no longer exists within the Trust due to organisational change, a successor team or individual will be identified and the log of records held in long-term storage will be transferred to them when the originating service is closed or dissolved or leaves the Trust.

Any commercial storage of confidential records must be subject to a contract with the supplier.

Appendix E – Providing Copy Letters to Service Users

Service users have a right to receive copies of any letters that help their understanding of their health and the care they are receiving and so these should be copied to them as of a right.

A letter includes communications between different health professionals, including:

- Letters or forms of referral from primary health care health professionals to other NHS services
- Letters from NHS health professionals to other agencies (e.g. social services)
- Letters to primary care from hospital consultants or other healthcare professionals following discharge or following an outpatient consultation or episode of treatment.

This policy does not relate to Care Plans which are covered by separate arrangements

Other documents, for example, single test results or Mental Health Act reports, should not normally be sent to service users. In due course, the outcome of such tests should be included in a letter that is copied to the service user.

Reports written to Mental Health Review Tribunals and Manager's Hearings should adhere to the guidance set out in the Mental Health Act.

Where there is frequent communication, the service user may choose not to have a copy of every letter.

Content of Letters - 'No surprises'

The contents of copied letters should reflect the discussion in the consultation with the healthcare professional sending the communication. There should be no new information in the letter which might surprise or distress the service user. All significant issues that have been discussed should be included in the letter.

Exclusions

There may be occasions where it would not be appropriate to copy letters to the service user, for example:

- Where it has been established that the service user does not want a copy
- Where the healthcare professional feels that it may cause harm to the service user
- Where the letter includes information about a third party who has not given consent
- Where special safeguards for confidentiality may be needed

Where the letter is written at the request of an outside agency, other factors apply in addition to whether the letter should be copied to the service user, for instance, compliance with data protection.

Harm to the service user

Sharing difficult or sensitive information is not in itself enough to justify not copying a letter even if the healthcare professionals is anxious to protect the feelings of the service user. It is the service user's choice as to whether they wish to receive a copy of the letter unless the health professional's judgement is that it would be likely to cause serious harm to the service user or some other person.

Third party information
It will not be appropriate to copy a letter which contains information about a third party (other than members of staff involved in the care of the service user), who has not given permission to disclose the information, unless the information was originally provided by the service user or is already known to them.

Consent to receive letters
It is for each service user to decide whether they wish to receive copies of letters written about them by health professionals. Service users should be routinely asked and their decision recorded.

It will be sufficient to seek consent once rather than each time a letter is written as long as it is explained at the start of an episode that copies of letters will be sent routinely to the service user unless they decide to opt out of receiving them, which can be done at any time.

The person responsible for generating the letter is responsible for ensuring that the service user's consent to receive copies is sought and for making and sending copies. This does not mean that this person is necessarily the person who carries out these activities.

Mental capacity
There will be no 'blanket' assumptions about mental capacity.

Whilst a person may lack capacity for one purpose, they may have sufficient capacity for another. These judgements will be made on a case-by-case basis.

Some people may not have mental capacity to make a decision about whether they would like a copy of their letter, for instance because they have a learning disability or dementia.

It should already be recorded on a service user's health record if they have someone to act on their behalf or to represent their views, for instance a carer, advocate etc. However, there is no formal legal provision underpinning such arrangements. Health professionals must use advice from their professional bodies and the DoH Good Practice in Consent Implementation Guide to ensure that arrangements are in the best interests of service users.

Copying letters to carers
Some service users have carers, for instance partners, friends or family members, who are actively involved in their care.

As carers, they need information and support from professionals supporting the person they care for, and they have a right to an assessment of their own needs. Service users may want to have information shared with their carers. With the service user's consent, a copy of letters can be sent to the carers. Occasionally the service user may not want a letter copied or shown to the carers. Both the service user and carer have the right to expect that information that either of them provides to the health service will not be shared with other people without their consent. In such circumstances, unless there is an over-riding reason to breach confidentiality, the wishes of the service user must be respected.

Children and young people
People over the age of 16 are able to make health care decisions for themselves, and should therefore, be asked for their agreement to receive copies of letters about them. It is up to healthcare professionals to assess the competence of younger children to understand and make a decision.

Letters written by non NHS agencies
Letters from non-NHS agencies may be written to healthcare professionals and not copied to service users. The healthcare professional may consider it is important to show the letter or give a copy to the service user. However, it is not the responsibility of the healthcare professional who receives the letter to send a copy to the service user.

Service users with a disability, impairment or sensory loss may require communications in specific formats – see the Accessible Information and Communication Policy on the SHSC Intranet for further details.

Appendix F – Recording of Gender Change on the EPR

Background

Once a person has been granted a Gender Recognition Certificate, information about their application for a certificate and about their previous gender becomes "protected information". It is an offence for a person who has acquired protected information in an official capacity to disclose the information to any other person, unless the subject of the protected information has agreed to the disclosure.

It is not an offence to disclose the 'protected information' referred to under the Gender Recognition Act 2004 if:

- the disclosure is made for medical purposes to a health professional; and
- the person making the disclosure reasonably believes that the subject has given consent to the disclosure or cannot give such consent.

'Medical purposes' includes the purposes of preventative medicine, medical diagnosis and the provision of care and treatment.

The NHSx Records Management Code of Practice states:

Any patient or service user can request that their gender be changed in a record by a statutory declaration, but the Gender Recognition Act 2004 provides additional rights for those with a GRC. The formal legal process (as defined in the Gender Recognition Act 2004) is that a Gender Reassignment Panel issues a Gender Reassignment Certificate. At this time a new NHS number can be issued, and a new record can be created, if it is the wish of the patient or service user. It is important to discuss with the patient or service user what records are moved into the new record and to discuss how to link any records held in any other health or care settings with the new record, including editing previous records to remove names, gender references or details. The content of the new record will be based on explicit consent under common law.

However, it is not essential for a transgender person to have a GRC in order to change their name and gender in their patient record and receive a new NHS number. They do not need to have been to a Gender Identity Clinic, taken any hormones, undergone any surgery, or have a Gender Recognition Certificate.

Process for recording change of gender on the EPR

Where a service user decides that they wish to identify as a different gender but does not have a Gender Recognition Certificate their electronic record will be updated with the new details and the old details stored in history without creating a new record.

Where a service user is formally granted a Gender Recognition Certificate they will be informed by the treating service of their right to have a new record created under their new identity and the old one closed. The risks to their continuity of care of not maintaining a link with the original record will be explained to the service user and their decision sought.

Where the service user opts to maintain a single, continuous record their name, gender and other details will be updated as appropriate on the EPR record and the old name will be stored in name history.

Where the service user opts for a new record the following process will be followed:

The treating service will inform the Information Department to ensure that the name of the existing client record is changed to an alias and any current episodes are closed.

A new EPR record will be created under the new service user details including the NHS number corresponding to these details. Where the service user has retained their original NHS number this will be recorded under the new record and removed from the old record. Where a new number has been issued the old number can be retained on the old client record but no link between the two will be maintained. Where the new record begins with the original NHS number but a new one is subsequently issued the EPR record will be updated with the new NHS number.

Any SHSC services currently involved in the service user's care will be informed to access the new record and NHS number by the person creating the new record. New referrals/episodes will be created for current services against the new client record. Records, notes etc will not be transferred from the old record to the new one without the service user's agreement.

A warning will be entered on EPR against the old record along the lines of:

"These records are protected under law and are actively audited. Do not access them without contacting the Data Protection Officer."

Appendix G – Access to Records held by Sheffield Archives

Some old patient records from Middlewood Hospital (formerly the West Riding Asylum and Wadsley Mental Hospital), have been transferred to the Sheffield Archives for permanent preservation, having been judged to be of historical interest.

No further patient records will be transferred to Sheffield Archives – the Records Management Code of Practice covers the transfer of records to a place of deposit for permanent preservation and clarifies that patient records should only be transferred where certain factors apply such as their relevance to peculiar local conditions, or significant local or national issues, or the development of new or unusual treatments.

UK GDPR and DPA 2018 do not apply to the records of deceased people but patient confidentiality still applies to the records held by Sheffield Archives, and Sheffield Health & Social Care is still the data controller in respect of these records.

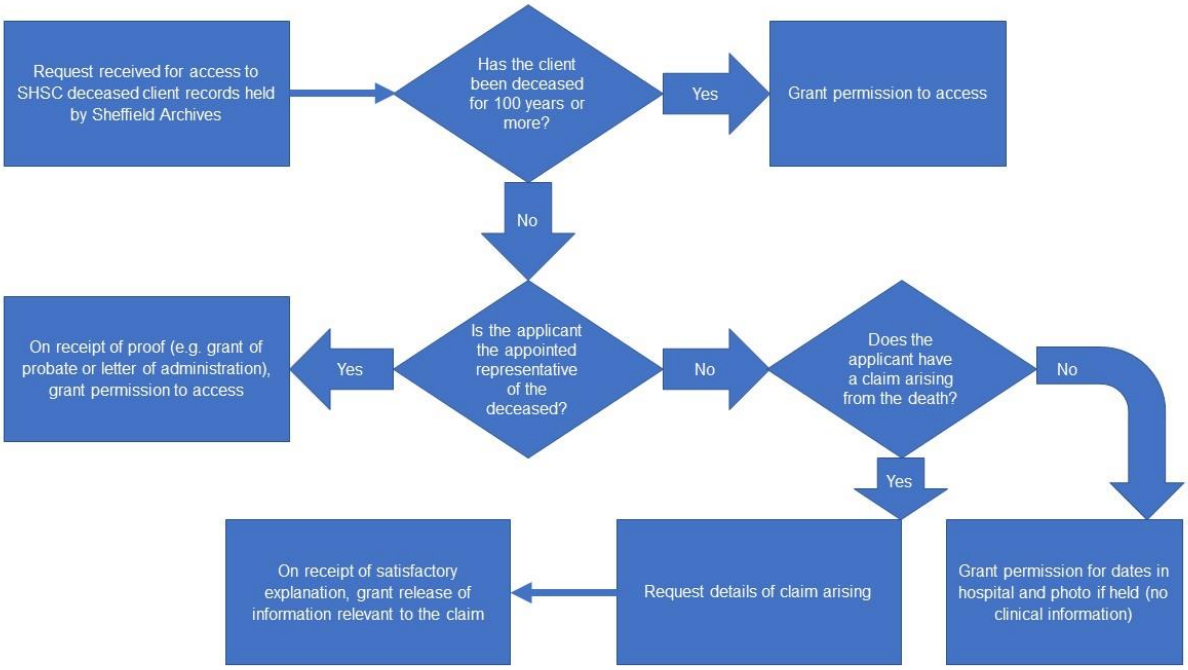
When Sheffield Archives receive requests to access the records (usually for genealogy purposes), these are referred to the SHSC Data Protection Officer for permission.

Access to records of deceased people is governed by the Access to Health Records Act 1990 – requests may be made by the appointed representative of the deceased or people who have a claim arising out of the death.

For other people who wish to access patient records held by Sheffield Archives, access to detailed patient information will not normally be granted until 100 years have passed since the death of the patient, or the date of the last entry in the record where the date of death is not known.

The Trust will allow confirmation of the dates the patient was treated and where a photograph of the patient is held a copy may be provided to applicants. Proof of relationship to the patient will not be required.

Any requests to deviate from these arrangements would need the approval of the Caldicott Guardian.


Request received for access to SHSC deceased client records held by Sheffield Archives
Has the client been deceased for 100 years or more?
Yes
Grant permission to access
No
On receipt of proof (e.g. grant of probate or letter of administration), grant permission to access
Yes
Is the applicant the appointed representative of the deceased?
No
Does the applicant have a claim arising from the death?
No
Yes
On receipt of satisfactory explanation, grant release of information relevant to the claim
Request details of claim arising
Grant permission for dates in hospital and photo if held (no clinical information)