Health Records Management Policy

POLICY

Reference	GV 007		
Approving Body **Date Approved**	Data Protection & Cyber Security Committee *June 2026*		
For publication to external SFH website	**Positive confirmation received from the approving body that the content does not risk the safety of patients or the public:**		
	YES	**NO**	**N/A**
	X		
Issue Date	*September 2026*		
Version	9		
Summary of Changes from Previous Version	Updated onto new template, updated EIA, updated current operational processes Data Security Incidents: Response, Escalation and Learning Access controls Legal Hold and Preservation of Records		
Supersedes	*8*		
Document Category	• *Information Governance*		
Consultation Undertaken	Information Governance Working Group Data Protection & Cyber Security Committee		
Date of Completion of Equality Impact Assessment	20/02/2026		
Date of Environmental Impact Assessment (if applicable)	Not applicable		
Legal and/or Accreditation Implications	• Public Records Act 1958 • Data Protection Act 2018 • Freedom of Information Act 2000 • NHS Code of Practice: Records Management 2021 • Caldicott2 Review of Patient Identifiable Information 2012 • Common Law Duty of Confidentiality • Working Together for Safeguarding Children 2018 • Access to Health Records Act (1990)		
Target Audience	All staff		
Review Date	1 years		
Sponsor (Position)	Chief Medical Officer/ Caldicott Guardian		
Author (Position & Name)	Head of Data Security & Privacy		

Lead Division/ Directorate	Corporate
Lead Specialty/ Service/ Department	Data Protection & Cyber Security
Position of Person able to provide Further Guidance/Information	Head of Data Security & Privacy, Data Protection Team

Associated Documents/ Information	**Date Associated Documents/ Information was reviewed**
Template control	April 2024

CONTENTS

Item	Title	Page
1.0	INTRODUCTION	4
2.0	POLICY STATEMENT	5
3.0	DEFINITIONS/ ABBREVIATIONS	10
4.0	ROLES AND RESPONSIBILITIES	10
5.0	APPROVAL	12
6.0	DOCUMENT REQUIREMENTS	12
7.0	MONITORING COMPLIANCE AND EFFECTIVENESS	21
8.0	TRAINING AND IMPLEMENTATION	22
9.0	IMPACT ASSESSMENTS	23
10.0	EVIDENCE BASE (Relevant Legislation/ National Guidance) and RELATED SFHFT DOCUMENTS	23
11.0	KEYWORDS	24
12.0	APPENDICES	24

APPENDICIES

Appendix 1	Medical Records Keeping Standards	25
Appendix 2	Data Security and Protection Toolkit (DSPT) and National Data Guardian (NDG) Standards Alignment	27
Appendix 3	Equality Impact Assessment	35

1.0 INTRODUCTION

Health records are a valuable resource because of the information they contain.

High quality information underpins the delivery of high-quality-based health care, and many other key service deliverables. Information is of greatest value when it is accurate, up to date and accessible when needed. A health records management service ensures that information is effectively managed and available when needed.

The benefits of effective records management are:

- Protecting business critical records and improving business resilience
- Ensuring information can be found and retrieved quickly and efficiently
- Complying with legal and regulatory requirements
- Reducing risk for litigation, audit and investigations
- Minimising storage requirements and reducing costs.

All NHS records are public records under the Public Records Act of 1958. They must be kept in accordance with statutory and NHS guidelines, including:

- Public Records Act 1958
- Data Protection Act 2018
- UK GDPR
- Freedom of Information Act 2000
- NHS Code of Practice: Records Management 2021
- Caldicott2 Review of Patient Identifiable Information 2012
- Common Law Duty of Confidentiality
- Working Together for Safeguarding Children 2018
- Access to Health Records Act (1990)

This policy states how health records will be managed within Sherwood Forest Hospitals NHS Foundation Trust.

Complying with the following legislative requirements and DoH Guidance:

- The Data Protection Act and the revised General Data Protection Regulations Principle Article 5 (e) in that patient data shall only be kept for as long as required to provide a patient with healthcare
- Records Management Code of Practice
- Data Security & Protection Toolkit
- Care Quality Commission
- Public Records Acts.

This Policy is issued and maintained by the Caldicott Guardian (the sponsor) on behalf of the Trust, at the issue defined on the front sheet, which supersedes and replaces all previous versions.

The primary purpose of keeping health records is for patient care. The record should detail of the investigation, diagnosis, treatment and subsequent outcomes for the benefit of the patient and healthcare professional involved in providing care

2.0 POLICY STATEMENT

This policy applies to all patient identifiable health records and patient identifiable clinical information, held by the Trust in its capacity of Data Controller. It includes information in all media formats including paper and digital records held in IT systems, maintained by the Trust including Digital Services or by clinical or ancillary departments.

By adopting this policy, the Trust aims to comply with data protection legislation in that 'personal data shall be kept in a form which permits identification of data subjects no longer than is necessary for the purposes for which the personal data is processed'.

The Sherwood Forest Hospitals NHS Foundation Trust, Board of Directors acknowledges the importance of health records and is committed to create, keep, make available to those entitled to access, maintain, and dispose of records, commensurate with legal, operational and information needs.

This policy relates to the management of health records and filing within medical case notes held by the Trust and used within the local health community at King's Mill, Newark and Mansfield Community Hospitals.

Records created in the course of the business of the Trust are public records under the term of the Public Records Act.

This policy forms part of and should be read in conjunction with a framework of Data Protection & Security policies, procedures, standards, and guidance.

This policy does not address in detail the retention and ultimate destruction (or permanent preservation) of records. These matters are covered by the sperate complementary Retention and Destruction Policy.

This policy does not address the management of corporate and administrative records. These records are covered by the separate complementary Corporate Records Policy.

Accountability

The Trust Board retains ultimate accountability for Health Records Management with executive responsibility delegated to the Caldicott Guardian and Senior Information Risk Owner (SIRO). They are supported operationally by the Head of Data Security and Cyber.

The Trust requires that adequate records are maintained to account fully and transparently for all actions and decisions, in particular:

- To ensure a full record of assessments, observations, care provided and outcomes to facilitate delivery of patient care
- To protect legal and other rights of patients and staff or those affected by those actions.
- To facilitate audit or examination.
- To provide credible and authoritative evidence if required by law.

Quality

The Trust requires that records are complete and accurate and the information they contain is reliable, relevant, fit for purpose and its authority can be guaranteed.

Accessibility

The Trust expects records, and the information they contain can be efficiently retrieved by those with a legitimate right of access, for as long as the records are held.

Training

The Trust requires all staff who are responsible for record-keeping to be made aware of their responsibilities through generic and Data Security protection specific mandatory training program and guidance.

Security

There is an expectation that records will be kept secure at all times and only released and accessed by staff who have the right to access them. Staff that regularly use medical records are responsible for their safe keeping and security. They must be protected from unauthorised changes or deletion, with controlled access and disclosure, and all activity tracked by audit trails and system logs. Records will be held in a robust format that remains readable for as long as the records are required.

Data Security Incidents: Response, Escalation and Learning

All actual or suspected incidents relating to the confidentiality, integrity or availability of health records must be treated seriously and managed in line with Trust incident reporting procedures.

A Data Security incident may include, but is not limited to:

- Loss or misplacement of paper health records
- Inappropriate access to health records
- Disclosure of records in error
- Failure to securely dispose of records
- Integrity or corruption issues affecting digital records

Incident Identification and Reporting

- All staff have a personal responsibility to identify and report any actual or suspected health record–related incidents or near misses as soon as they are identified.
- Incidents must be reported using the Trust's approved incident reporting system Datix in accordance with the incident reporting policy.
- Deliberate failure to report an incident may result in management action.

Incident Assessment and Investigation

- All reported incidents involving health records will be triaged, risk-assessed and investigated proportionately by the Data Protection Team in collaboration with relevant Information Asset Owners (IAOs).
- Where required, incidents will be escalated to the:
  - Senior Information Risk Owner (SIRO)
  - Caldicott Guardian
  - Data Protection Officer
- Incidents meeting external reporting thresholds will be managed in line with statutory requirements, including reporting to the Information Commissioner's Office (ICO) where applicable.

Learning, Corrective Action and Improvement

- The Trust is committed to a just culture approach to incident management, focusing on learning and system improvement rather than individual blame.
- Root cause analysis will be used to identify:
  - Contributory factors
  - Control weaknesses
  - Opportunities to prevent recurrence
- Corrective actions may include:
  - Process redesign
  - Policy clarification
  - Targeted training or awareness activity
  - Technical or administrative controls
- Learning from incidents will be:
  - Shared through Information Governance structures

- Used to inform policy updates, training content and risk management
- Monitored for implementation and effectiveness

Governance Oversight and Assurance

- Health record–related incidents, trends and learning outcomes are reviewed regularly by:
- Information Governance Working Group
- Data Protection & Cyber Security Committee
- Incident data is analysed to identify themes, emerging risks and assurance gaps, supporting continuous improvement and Board-level assurance.

Access Control, Review and Removal of Access

The Trust operates a role-based access control approach to health records to ensure that only authorised individuals with a legitimate business or clinical need can access patient and service user information.

Access to health records must:

- Be approved, proportionate, and limited to the minimum necessary
- Reflect the user's current role, responsibilities and level of involvement in care or service delivery
- Be subject to regular review and prompt removal where no longer required

Granting and Modifying Access

- Access to health records is granted only with appropriate Information Asset Owner (IAO) approval and in accordance with Trust account management procedures.
- Where an individual changes role, department or duties, their access must be reviewed and updated without delay to ensure it remains appropriate.
- It is not acceptable for staff to retain access based on historic roles or previous responsibilities.

Routine Access Reviews

- Regular access reviews must be undertaken for systems and records holding patient identifiable information.
- Reviews must confirm that:
- Users still require access
- Access levels remain appropriate
- Any unnecessary, excessive or inappropriate access is removed

- Reviews must be documented and retained to provide evidence for audit, DSPT assurance and regulatory inspection.

Immediate Removal of Access

Access to health records must be removed or suspended promptly when:

- A staff member leaves the organisation
- A contract, placement or temporary role ends or expires
- An individual no longer requires access due to role change or redeployment
- There is an actual or suspected information governance incident
- There is a concern regarding misuse, inappropriate access or risk to patient information

Line managers and IAOs are responsible for ensuring leaver, mover and suspension processes are initiated in a timely manner.

Monitoring, Assurance and Escalation

- Access controls and review outcomes are subject to monitoring and audit through data security and cyber assurance processes.
- Any failure to review or remove access appropriately will be treated as a Data Security risk and may be managed through incident reporting, risk registers and escalation to:
  - Information Asset Owners
  - Senior Information Risk Owner (SIRO)
  - Data Protection & Cyber Security Committee
- Repeated or serious failures may result in additional controls, targeted training or formal management action.

Learning and Continuous Improvement

Access-related incidents, near misses or audit findings will be reviewed to identify system weaknesses and learning opportunities.

- Learning will be used to:
  - Strengthen processes and controls
  - Inform staff training and awareness
  - Improve integration between HR, IT and Information Governance functions

Evidence, Assurance and Audit Trail for Access Control

The Trust maintains a clear evidence-based assurance framework to demonstrate that access to health records is regularly reviewed, appropriately removed and effectively governed.

3.0 DEFINITIONS/ ABBREVIATIONS

The Policy	means Health Records Management Policy
The Trust	means Sherwood Forest Hospitals NHS Foundation Trust
Caldicott Guardian	individual appointed by the Chief Executive responsible for protecting patient information. This includes ensuring the protection of patient records and that appropriate standards are maintained and monitored.
'SIRO'	Senior Information Risk Owner; responsible for leading and implementing the information risk management process and providing the Board assurance.
'IAO'	Information Asset Owner; responsible for understanding and assessing the information they 'own' and providing the SIRO with assurance in relation to the security of that asset.
'IAA'	Information Asset Administrator: responsible for providing support to their IAOs ensuring that IG policies are followed and that information risks and incidents are documented and escalated accordingly.
Disposal and destruction	means by which notes are removed from file, checked, disposed of, and destroyed.

4.0 ROLES AND RESPONSIBILITIES

Committees

Data Protection & Cyber Security Committee (DPCSC)

DPCSC is responsible for ensuring that Data Protection policies, principles and standards including those relating to records management are implemented and understood within the organisation.

The DPCSC will authorise the destruction of source health records bi-monthly by reviewing quality assurance level reports and completing a disposal form retained as a disposal record.

DPCSC are also responsible for:

- Promotion of a culture of excellence in record keeping and records management
- Monitoring compliance and effectiveness of this policy
- Evaluation and approval of applications for permanent or extended retention of records.

- Assessing risk, reviewing quality assurance reports and authorising the destruction of source health records/documents post scanning.

Individual Officers

The Trust Board and Chief Executive

The Trust Board recognises that it has a specific corporate accountability for ensuring records are managed and disposed of in a timely and confidential manner in accordance with legal, NHS guidance and data protection standards required by regulatory bodies. The Chief Executive has ultimate responsibility for compliance with this policy.

The Senior Information Risk Officer (SIRO)

The Trust has a Board Level Senior Information Risk Officer as required by the Data Security & Protection Toolkit. The SIRO takes ownership of the Trust's information risk policy, acts as advocate for information risk on the Board and provides written advice to the accounting officer on the content of their Statement of Internal Control regarding information risk.

The SIRO is responsible for developing and encouraging good information handling practice amongst all members of the Trust. This individual will work with other Trust Directors and Managers who have a remit which includes records and information management elements, either clinical or corporate.

The Caldicott Guardian

The Caldicott Guardian is responsible at Trust Board level for approving and ensuring that national and local policies on the handling of confidential personal information are implemented. The Caldicott Guardian also has the added responsibility for protecting the confidentiality of patient and service user information and enabling appropriate information sharing.

The Data Protection Officer

The DPO has a duty to ensure the Trust complies with data protection legislation. More specifically the DPO will monitor compliance with the GDPR principles and conduct internal audits, particularly in relation to Article 5e):

Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals.

The DPO is the first point of contact for the Information Commissioner's Office (ICO) and for patients who have concerns about the retention and disposal of their health records.

Directors as Information Asset Owners (IAOs) and Senior Managers

Directors and Senior Managers are expected to lead by example by promoting a culture which properly values, protects and uses data.

The responsibility for local records and information lifecycle management is devolved to Directors and Service Managers, Heads of Department/Professional leads who have overall responsibility for records and information generated by their services areas activities and specifically that:

- records are appropriately captured and retained in registered systems;
- the management and retention and disposal of records takes place in a timely and secure way within their areas of responsibility and in accordance with this policy;
- their staff receive training, are aware of the requirements of appropriate Information Governance/Governance policies and apply the correct procedures and controls relevant to their work.

IAO's have responsibility for providing assurance to the SIRO that information, particularly personal information, is effectively managed within their Directorate/ Department.

Information Asset Administrators (IAAs)

IAAs ensure that IG policies and procedures are followed, recognise actual or potential security incidents and take steps to mitigate those risks, consult their IAO on incident management, and ensure that information asset registers are accurate and up to date.

5.0 APPROVAL

This document has been circulated appropriately for comments to the following groups: Clinical Reference Group and the Information Governance Working Group, it has been updated accordingly and then approved by the Data Protection & Cyber Security Committee.

6.0 DOCUMENT REQUIREMENTS

This policy relates to the management of all health records of the Trust, including but not limited to:

- Patient health records (electronic or paper based; including those concerning all specialties)
- Records of private patients seen on NHS premises
- All registers e.g. birth registers, theatre registers, minor operations registers

- X-ray and imaging reports, outputs and images
- Photographs, slides and other images
- Microform (i.e. fiche / film)
- Audio and videotapes, cassettes and disks.
- Emails
- Digital records
- Computerised records
- Instant messaging

This policy relates to the management of health records and filing within medical case notes held by the Trust and used within the local health community at King's Mill, Newark, Mansfield Community and Ashfield Community Hospitals. It also provides general associated advice in relation to the retrieval, tracking, retention and destruction of paper case notes.

All records created in the course of the business of the Trust are public records under the terms of the Public Records Act.

Shared Clinical Records – between organisations providing you with care:

The Trust is part of an Integrated Care System (ICS) which shares patient information between providers. This is managed through the Notts Care Record.

The Notts Care Record is a secure, digital system in Nottingham and Nottinghamshire that shares patient information in real-time between health and care organisations, such as hospitals, GPs, and social care, to improve, speed up, and coordinate care. It enables authorised staff to view relevant medical histories, benefiting our patients through joined up care and reducing the need for patients to repeat information.

Only staff directly involved in a patient's care should access the records, with access logged for privacy protection, complying with UK GDPR and the Data Protection Act 2018.

Patients have the right to object to their data being available through the system, though this may impact care coordination.

Regulatory and Legal Framework

Under the terms of the Public Record Act 1958 all records created in the Trust are regarded as public records. The act imposes a statutory duty on the Trust to make arrangements for the safe keeping and eventual disposal of records. The ownership and copyright of records created within Trust lies with the Trust and not the individual who has created them.

As a Public Authority subject to the Freedom of Information Act (FOIA) the Trust has a duty to follow the Code of Practice for Records Management published by the Lord Chancellor in

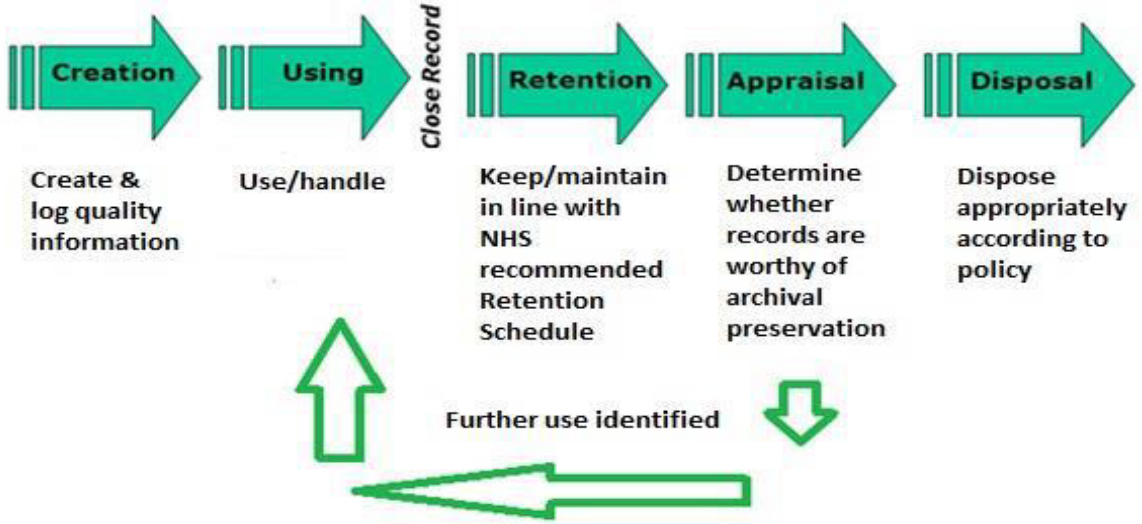
accordance with section 46 of the FOIA. The code provides guidance to public authorities on keeping, managing and destroying records.

The Data Protection Act sets in law how personal and sensitive information may be processed and largely influences the way we handle care records. Further guidance on the confidentiality aspects of record keeping is provided in the NHS Confidentiality Code of Practice and the Trust Data Protection and Confidentiality Policy.

The Records Management Code of Practice for Health and Social Care 2021 (updated 2023) provide records management guidance for NHS and Social Care organisations based on current legal requirements and professional best practice. The Trust is committed to following the guidance issued in the code of practice, and the procedures outlined in this policy are largely based on the guidance included in this Code of Practice.

The Records Information Lifecycle

The records or information lifecycle is a term that describes a controlled regime in which information is managed from the point that it is created to the point that it is either destroyed or permanently preserved as being of historical or research interest. The cycle is illustrated in figure 1



Procedural guidance associated with each stage of the cycle is included in subsequent sections

Record Creation

ISO 15489-1:2016 Information and Documentation – Records Management describes the characteristics of 'Authoritative Records' as being authentic, reliable integral and useable. Table 1 below expands on these definitions.

Table 1. Record Characteristics

Record Characteristic	How to Evidence
Authentic	It is what it purports (claims) to be To have been created or sent by the person purported to have created or sent it, and to have been created or sent at the time purported.
Reliable	Full and accurate record of the transaction/activity or fact created close to the time of transaction/activity created by individuals with direct knowledge of the facts, or by instruments routinely involved in the transaction /activity.
Integrity	Complete and unaltered, and protected against unauthorised alteration. Alterations after creation can be identified as can the persons making the changes.
Useable	Located, retrieved, presented and interpreted. The context can be established through links to other records in the transaction/activity.

By organising records in a file system or classification scheme elements of 'Metadata' are associated with each record which helps maintain the characteristics described above. Metadata in its simplest form would identify the creator, creation date and subject of a record but can be expanded to include additional information such as destruction date, identifiers and accessibility.

Classification schemes can be a simple arrangement of files and folders on a Network drive increasing in sophistication up to comprehensive Electronic Document and Records Management System.

All Trust records should be stored within an appropriate classification/filing system after creation. This will ensure they remain secure and accessible from the outset and be available to support Trust business activity.

Handling and Using Records

Record Keeping

When completing entries in or creating any form of records the following general guidance should be applied:

- Be factual, consistent and accurate
- Write clearly and in such a way that text cannot be erased
- Write in such a way that any alterations or additions are dated, timed and signed in such a way that the original entry can still be read.

The record must identify uniquely the individual who has provided the care and completed the record.

Healthcare professionals may be subject to additional record keeping codes of practice set by their professional bodies. The Academy of Medical Royal Colleges has published a set of generic medical record keeping standards which are reproduced at Appendix 1. All entries in Trust care records should conform to these standards.

Rights granted to members of the public by the Freedom of Information Act and to patients and staff under the Data Protection Act can result in copies of corporate records being placed in the public domain and data subjects obtaining copies of records containing information about them. Providing record entries are factual and accurate and personal records do not include any unnecessary and/or derogatory comments record disclosure should not create any additional issues. It is important that all those contributing to any record do so with a mind that it is likely that any written record can be accessed either under FOI legislation, or under Data protection legislation.

Confidentiality and Access

All Trust records are public records and thus are subject to a number of statutory provisions regarding confidentiality, access and disclosure. Patients entrust the NHS or allow it to gather sensitive information relating to their health and other matters as part of their seeking treatment. They do so in confidence and they have the legitimate expectation that staff will respect this trust. It is essential, if the legal requirements are to be met and the trust of patients is to be retained, that the NHS provides, and is seen to provide, a confidential service.

Specific guidance on patient confidentiality issues is provided in the Trust Data Protection and Confidentiality Policy. Further advice on all aspects of patient confidentiality and the application of the Data Protection Act (2018) on the way we handle records in the Trust can be obtained from the Trust Data Protection Team.

The Data Protection Act (2018) makes provision in law for ‘data subjects’ (e.g. patients and members of staff) to obtain copies or otherwise gain access to information held about them. The Trust Access to Records Policy covers this aspect of records management and further advice on the procedure can be obtained from the Trust Data Protection Team.

In 2000 the government introduced the Freedom of information Act providing members of the public with the general right of access to recorded information held by a wide range of bodies across the public sector. The effect of this legislation is to make it possible for people to obtain copies of a wide range of Trust records that in the past would have remained confidential. The Trust Freedom of Information Policy covers this aspect of records management, and further advice on the procedure can be obtained from the Trust Data Protection Team.

Record Tracking

Whilst a significant proportion of the medical records held within the Trust are accessed digitally, there are many areas which remain reliant on paper based medical records. With paper, it is essential that these are held with the principles of Confidentiality, Integrity and Availability in mind. To achieve this, the movement and location of all records should be controlled to ensure that a record can be retrieved at any time and there is an auditable trail of record transactions. This is best achieved using some form of record tracking system to record the movement of records between locations.

It is the policy of the Trust that patient health record folders are tracked using the Patient Administration System (PAS) record tracking component. Users must complete appropriate training before access is be granted to the user.

While electronic records do not require tracking as such, control must be exercised when hard copies are produced. If separate clinical case notes are produced from electronic systems to form a filing system, individual record movements should be tracked to aid retrieval and avoid loss of data.

For most areas, where movement of records is restricted, paper-based systems may be employed, using registers or tracer cards to record the relevant information.

When deciding to move records which contain personal or sensitive information to destinations external to the Trust (including archive storage) consideration needs to be given to security and confidentiality and a means of dispatch chosen that affords an adequate level of security. (See Trust Data Protection Policy for further guidance.)

Paper Record Storage

When not required for operational purposes paper records should be kept in a secure storage area. Records in current use should ideally be stored close to the point of use while records no longer in current use can be transferred to secondary or archive storage more remote from the operational area.

Records should be stored in an appropriate environment to ensure they remain fit for purpose during their expected period of retention. When evaluating the suitability of a location for record storage the following points should be considered:

- Environment. Is the location suitable for the type of material being stored? Is the area free from hazards that may cause the records to deteriorate or place at risk staff that may need to access the records? i.e. excessive dust, damp, restricted access.
- Security. Is the level of security offered by the location acceptable for the type of record being stored?
- Ease of Access. Can records be easily located and retrieved? Some restrictions on access may be acceptable for records that are not frequently recalled.

Layout. Consideration should be given to the design of the storage location to ensure the most cost-effective use is made of the space available.

External storage companies provide an alternative to local storage and in the short term can prove a cost-effective alternative in areas where record storage space is at a premium. The Trust has negotiated a contract for external record storage with SDS, with storage premises located in Nottinghamshire. The process for retrieval of records held off site is managed via the case notes store.

Records regarding the location and status of notes can be found in Careflow PAS.

A comprehensive log should be maintained of any records sent for commercial storage including a proposed date for review/destruction. A mechanism for reviewing these records for disposal should be developed and implemented to ensure records are not retained longer than necessary.

Digital Record Storage

Digital information should be stored in such a way that throughout the lifecycle it can be recovered in an accessible format. Over time such changes as migration to new formats can cause links to other documents and embedded documents to fail to open impacting the integrity of the record. Any changes to the electronic storage systems used to hold Trust records should only take place after full consideration of the impact on the records held, and successful testing of retrieval of transferred records from the new version/system.

Legal Hold and Preservation of Records

Where records may be relevant to a statutory inquiry, public inquiry, safeguarding review, police investigation, inquest, litigation, complaint, disciplinary process or any other formal proceeding, the Trust will implement a legal hold (preservation requirement).

Suspension of Disposal

All routine destruction, deletion or alteration of records must be immediately suspended where a legal hold applies or is reasonably anticipated. This applies regardless of whether records have reached their minimum retention period.

A legal hold applies to all records held by the Trust, in any format, including:

- Electronic patient records and system data
- Paper health records and archived files
- Emails, instant messages and other communications
- Audio, video and scanned records
- Metadata, audit trails and system logs

Identification and Notification

The Data Protection Team, Records Management function and/or Legal Services will:

- Identify affected record types, systems and locations
- Issue clear instructions to relevant Information Asset Owners (IAOs), managers and staff
- Maintain a documented record of the legal hold, including scope, rationale and implementation date

Responsibilities

All staff, IAOs and managers must:

- Preserve all records within their control that may fall within scope
- Not delete, amend, overwrite or otherwise dispose of relevant records
- Escalate any uncertainty, risks or potential breaches to the Data Protection Team without delay

Controls and Assurance

Where practicable, technical and administrative controls will be implemented to:

- Prevent deletion or modification of affected records
- Restrict access where necessary
- Ensure audit trails demonstrate preservation and control

Compliance with legal hold requirements will be subject to monitoring through audit, incident reporting and governance oversight via Information Governance structures.

Release of Legal Hold

Records subject to legal hold will only be returned to normal retention and disposal processes when:

- Formal confirmation is provided by the Data Protection Team and/or Legal Services, and
- It is confirmed that the preservation requirement no longer applies

Non-Compliance

Failure to comply with a legal hold may result in disciplinary action and may expose the Trust to legal, regulatory and reputational risk.

7.0 MONITORING COMPLIANCE AND EFFECTIVENESS

Minimum Requirement to be Monitored (WHAT – element of compliance or effectiveness within the document will be monitored)	Responsible Individual (WHO – is going to monitor this element)	Process for Monitoring e.g. Audit (HOW – will this element be monitored (method used))	Frequency of Monitoring (WHEN – will this element be monitored (frequency/ how often))	Responsible Individual or Committee/ Group for Review of Results (WHERE – Which individual/ committee or group will this be reported to, in what format (eg verbal, formal report etc) and by who)
Compliance with record handling and best practice	Data Protection Team and IAA's within each division	Incidents reported with record related causes	Ongoing	Information Governance Working Group, Clinical Reference Group, Data Protection & Cyber Security Committee via a report, CSTO Divisional Governance.
Medical Record Storage Areas	Data Protection Team IAOs within each department/division CSTO DLT	Spot check audits Completion of audits on AMAT	Ongoing	Information Governance Working Group, Clinical Reference Group, Data Protection & Cyber Security Committee via a report, CSTO Divisional Governance.

Monitoring adherence to this policy is the responsibility of the DPCSC. Data Protection Policies and procedures are subject to regular programmes of both internal and external audit reported via these committees, and all required actions are ongoing. When monitoring identifies deficiencies action plans will be developed to address them.

8.0 TRAINING AND IMPLEMENTATION

Retention and Disposal as an aspect of Records Management features within Data Protection Training which all staff complete annually.

All staff that are responsible for record-keeping are made aware of their responsibilities through generic and Data Protection & Security specific mandatory training programs and guidance. Similarly, all staff are made aware of their filing responsibilities through mandatory and induction training programs and guidance. It is the responsibility of Departmental Managers to deliver such training although mandatory training is provided online, and all patient administration staff are required to complete this annually.

The following groups of staff will be appropriately trained in the following aspects of case note management:

Training	Staff Group
• Storage and security • Notes retrieval and tracking • Filing within case notes	• Case Note Store Staff • Records Assistants • Endoscopy Administrative Staff • Ward clerks/receptionists • Clinical Coding staff • Pathway Co-ordinators • Clinical Typists • Outpatient Receptionists • Waiting list Clerks • Pre-Operative Assessment Clerks • Cardio – respiratory Clerks • Central Booking Clerks
• Storage and security • Notes retrieval and tracking • Filing within case notes • Retention and destruction	• Archivists
• Storage and security	• All staff groups (via mandatory online training module)

Training in all aspects of this policy is included in an online training package available in the Sherwood Forest Training Academy. Records of such training will be maintained by the training and Development Department for all patent administration staff for whom this is considered mandatory. Additional training may be required when the policy is amended, and the online training package may require an update.

Destruction and disposal of records is only to be carried out by the appropriately trained staff (archivists) in the Case Note Store on both the King's Mill and Newark sites. Staff destroying notes or sending them for offsite storage should follow the Weeding and Destruction SOP and Retention and Destruction policy.

Divisional General Managers are to ensure that staff groups detailed above:

- Complete the mandatory training. Details of those attending said training will be provided to Divisional General Mangers by the Training and Development Department in order to monitor compliance.
- Training requirements can be monitored. They will also be required to ensure that these staff groups undertake Data Protection & Security mandatory training on an annual basis. They will ensure that those staff who use case notes are trained in the case note tracking process or are aware of how they can arrange for notes to be tracked when required.

Divisional Information Asset Owners are to identify needs for awareness training for any other staff groups within their Division as required. Identified needs will be supported by the Data Protection Team and Case Note Store managers as appropriate.

9.0 IMPACT ASSESSMENTS

- This document has been subject to an Equality Impact Assessment, see completed form at Appendix 1
- This document is not subject to an Environmental Impact Assessment

10.0 EVIDENCE BASE (Relevant Legislation/ National Guidance) AND RELATED SFHFT DOCUMENTS

Evidence Base:

- This Policy has been developed with reference to:
- Public Records Act 1958 and 1967
- Data Protection Act 2018
- Freedom of Information Act 2000
- Access to Health Records Act 1990
- Caldicott2 Review of Patient Identifiable Information 2012
- Common Law Duty of Confidentiality
- A Clinician's Guide to Record Standards Part 2 published by the Academy of Medical Royal Colleges.
- NHSLA Risk Management Standards (Standard 1, Criterion 7)
- NHS Data Security and Protection Toolkit
- Records Management Code of Practice for health and social care 2016

National Guidance

- Records Management Code of Practice for Health and Social Care 2016
- Health Archives Group: Hospital Patient Case Records - A Guide to their Retention and Disposal
- Data Security and Protection Toolkit Requirements

Legislation

- Data Protection Act, and post May 2018 the revised General Data Protection Regulations
- Public Records Act 1958, 1967 & National Guidelines

Related SFHFT Documents:

This policy is to be used in conjunction with the following complementary policies and procedures:

- Procedures for the Management of medical Records /SFH Case Notes and associated processes
- Retention and Destruction Policy
- Information Security Policy
- Information Governance Policy
- Information Sharing Protocol
- Internet and Email Policy
- Freedom of Information Policy
- Access to Health Records Procedures
- Clinical Record Keeping Standards Policy
- Confidentiality Policy
- Subject Access policy
- Safe haven Policy
- Alert Policy
- Adoption Policy (in development)

11.0 KEYWORDS

- Weeding
- Destruction
- UK GDPR
- Data Protection Act

12.0 APPENDICES

- Appendix 1 – Medical Records Keeping Standards
- Appendix 2 - Data Security and Protection Toolkit (DSPT) and National Data Guardian (NDG) Standards Alignment
- Appendix 3 – EIA Impact Assessment Form

Appendix 1

Medical Records Keeping Standards

Medical Record Keeping Standards Standard Number	Description
1	The patient's complete medical record should be available at all times during their stay in hospital
2	Every page in the medical record should include the patient's name, identification number (must include NHS number, may include local ID) and location in the hospital
3	The contents of the medical record should have a standardised structure and layout
4	Documentation within the medical record should reflect the continuum of patient care and should be viewable in chronological order
5	Data recorded or communicated on admission, handover and discharge should be recorded using a standardised proforma
6	Every entry in the medical record should be dated, timed (24 hour clock), legible and signed by the person making the entry. The name and designation of the person making the entry should be legibly printed against their signature. Deletions and alterations should be countersigned, dated and timed27
7	Entries to the medical record should be made as soon as possible after the event to be documented (for example change in clinical state, ward round, investigation) and before the relevant staff member goes off duty. If there is a delay, the time of the event and the delay should be recorded
8	Every entry in a medical record should identify the most senior healthcare professional present (who is responsible for decision making) at the time the entry is made
9	On each occasion a transfer of care occurs, the consultant responsible for the patient's care will change the name of the responsible consultant and the date and time of the agreed transfer of care
10	An entry should be made in the medical record whenever a patient is seen by a doctor. When there is no entry in the hospital record for more than four (4) days for acute medical care or seven (7) days for

	long-stay continuing care, the next entry should explain why.
11	The discharge record/discharge summary should be commenced at the time a patient is admitted to hospital
12	Advanced Decisions to Refuse Treatment, Consent, and Cardiopulmonary Resuscitation decisions must be clearly recorded in the medical record. In circumstances where the patient is not the decision maker, that person should be identified e.g. Lasting Power of Attorney

Appendix 2 - Data Security and Protection Toolkit (DSPT) and National Data Guardian (NDG) Standards Alignment.

Purpose

This appendix demonstrates how the Health Records Management Policy supports compliance with:

- The **Data Security and Protection Toolkit (DSPT)** mandatory assertions
- The **National Data Guardian's 10 Data Security Standards**

Together, these provide the national framework for protecting patient information and assuring the Board, regulators and the public that health records are managed securely and lawfully.

DSPT Mandatory Assertions – Policy Alignment

DSPT Assertion 1.1 – Lawful, fair and transparent processing

"Personal data is processed lawfully, fairly and transparently in line with data protection legislation."

Policy alignment:
This policy establishes lawful handling of health records in accordance with the UK GDPR, Data Protection Act 2018, Common Law Duty of Confidentiality and Caldicott Principles, ensuring transparency via Trust privacy notices and supporting IG policies.

DSPT Assertion 1.2 – Security of personal data

"Personal data is protected against unauthorised or unlawful processing and against accidental loss, destruction or damage."

Policy alignment:
The policy mandates secure storage, controlled access, record tracking, audit trails and system logs for both paper and digital records, safeguarding confidentiality, integrity and availability.

DSPT Assertion 2.1 – Data minimisation and retention

"Personal data is adequate, relevant, limited to what is necessary and retained in line with defined retention schedules."

Policy alignment:
The policy enforces compliance with the Records Management Code of Practice for Health and Social Care and the Trust Retention and Destruction Policy, ensuring records are retained only as long as necessary and disposed of securely.

DSPT Assertion 3.1 – Senior Information Risk Owner (SIRO)

"A Senior Information Risk Owner (SIRO) is in place and actively manages information risks."

Policy alignment:
The SIRO holds Board-level accountability for information risk and provides assurance regarding the management of health records.

DSPT Assertion 3.2 – Information Asset Owners (IAO's)

"Information Asset Owners understand and manage the risks to the personal data and information assets they own."

Policy alignment:
IAOs and IAAs are responsible for the secure management of records and information assets within their remit and provide assurance through asset registers and risk management processes.

DSPT Assertion 4.1 – Training and awareness

"Staff complete annual data security and data protection training and understand their responsibilities."

Policy alignment:
All staff complete mandatory annual training, with additional role-specific training for those managing health records.

DSPT Assertion 5.1 – Data Security incidents

"Data security incidents and near misses are identified, reported, investigated and managed appropriately."

Policy alignment:
The policy supports reporting, investigation and escalation of all record-related incidents via Trust information governance and corporate governance processes.

DSPT Assertion 6.1 – Data sharing and secondary uses

"Data sharing and secondary uses of personal data are lawful, justified, transparent and subject to appropriate controls."

Policy alignment:
Data sharing through approved systems (e.g. Notts Care Record) operates under role-based access, auditing and patient choice arrangements, including application of the National Data Opt-Out where required.

National Data Guardian (NDG) Data Security Standards – Policy Alignment

This policy also supports compliance with the National Data Guardian's 10 Data Security Standards, as follows:

NDG Standard 1 – Personal confidential data is handled lawfully

Supported through compliance with UK GDPR, DPA 2018, Caldicott Principles and clearly defined access controls.

NDG Standard 2 – Staff understand their responsibilities

Mandatory annual training and role-specific records management training ensure staff understand how to handle health records securely.

NDG Standard 3 – Clear policies and processes

This policy provides clear, accessible guidance on record creation, handling, retention and disposal across all formats.

NDG Standard 4 – Access is on a need-to-know basis

Role-based access controls and tracking ensure staff only access records necessary for their duties.

NDG Standard 5 -Process review and improvement

Compliance monitoring, audits and incident reviews drive continuous improvement in records management practices.

NDG Standard 6 – Responding to incidents

Processes are in place to detect, report, investigate and learn from data security incidents and near misses.

NDG Standard 7 – Continuity planning

Secure storage, tracking and lifecycle management of records supports operational resilience and continuity of care.

NDG Standard 8 – Supplier assurance

Where records are stored or managed by third parties, contractual and governance controls ensure equivalent data security standards.

NDG Standard 9 – Physical and technical security

Appropriate physical security for paper records and technical safeguards for digital records are mandated.

NDG Standard 10 – Cyber and system assurance

Electronic records are protected through secure systems, access logging, monitoring and aligned cyber security controls.

CAF-aligned DSPT mapping (Cyber Assessment Framework outcomes)

The DSPT is aligned to the National Cyber Security Centre (NCSC) Cyber Assessment Framework (CAF). The table below maps relevant parts of the Health Records Management Policy to CAF outcomes, indicating where the policy contributes to meeting each outcome (supported by local procedures, technical controls and evidence).

CAF objective	Outcome	Outcome focus (summary)	Related NDG standard(s)	How this policy supports the outcome (examples)
A. Managing security risk	**A1.a**	Governance, roles and responsibilities are defined and understood.	NDG 3; NDG 5	Defines accountability for records management and information risk (e.g., Board-level SIRO accountability, IAOs/IAAs responsibilities) and requires adherence to Trust IG policies and supporting procedures.
A. Managing security risk	**A1.b**	Appropriate policies and processes are in place to manage security risk.	NDG 3; NDG 9	Sets requirements for secure creation, handling, storage, tracking, access control, retention and secure disposal of health records (paper and digital), aligned to UK GDPR/DPA 2018, confidentiality duties and relevant codes of practice.
A. Managing security risk	**A1.c**	Security risk management is integrated into business processes and decision-making.	NDG 5	Requires records to be managed as information assets with assurance via registers, audits, incident review and governance oversight (e.g., IG Working Group / Data Protection & Cyber Security Committee).

B. Protecting against cyber attack	**B2.a**	Identity and access control prevents unauthorised access to systems and data.	NDG 4; NDG 9	Mandates controlled/role-based access to records and systems, need-to-know principles, and record tracking for physical records to reduce inappropriate access.
B. Protecting against cyber attack	**B2.b**	Users and administrators are managed securely (e.g., appropriate permissions).	NDG 4; NDG 9	Supports least-privilege access by defining who may access records and under what conditions; requires that access is auditable and governed through Trust access management arrangements.
B. Protecting against cyber attack	**B3.a**	Data is protected in storage and handling (including physical protection where applicable).	NDG 9	Requires secure storage for paper records and technical safeguards for electronic records, including controls to protect confidentiality, integrity and availability throughout the records lifecycle.
B. Protecting against cyber attack	**B4.a**	Activities that can introduce cyber risk are governed (e.g., third parties/suppliers).	NDG 8	Where records are stored/processed by third parties, requires contractual/governance controls to ensure equivalent standards (supports supplier assurance expectations).
C. Detecting cyber security events	**C1.a**	Monitoring is in place to detect abnormal events and potential security incidents.	NDG 10; NDG 5	Supports the use of audit trails, tracking and (where applicable) access logging for electronic records; enables monitoring and review to identify inappropriate access or loss.

D. Minimising the impact of incidents	**D1.a**	Effective response processes exist for security incidents and near misses.	NDG 6	Requires reporting, investigation and escalation of record-related incidents through Trust IG/corporate governance processes, supporting timely containment and learning.
D. Minimising the impact of incidents	**D2.a**	Continuity arrangements support recovery and safe service delivery.	NDG 7	By requiring secure storage, tracking and lifecycle controls, supports availability of records for continuity of care; aligns with local business continuity arrangements for records access (paper/digital).
E. Using and sharing information appropriately	**E1.a**	Data is used and shared lawfully, fairly and transparently.	NDG 1	Sets lawful bases and confidentiality expectations and references transparency mechanisms (e.g., privacy notices) for the handling and sharing of patient information.
E. Using and sharing information appropriately	**E2.a**	Information sharing and secondary use is controlled and audited.	NDG 1; NDG 4; NDG 10	Requires that sharing occurs via approved systems and arrangements (e.g., role-based access and auditing), supports patient choice controls (including National Data Opt-Out where applicable) and appropriate approvals for secondary use.

Note: This mapping is indicative and focuses on where the Health Records Management Policy contributes to each CAF outcome. Full DSPT evidence typically also includes supporting procedures, technical configurations (e.g., access management, logging/monitoring), training records, audit results and incident response documentation.

Monitoring, Assurance and Evidence

Compliance with DSPT assertions and NDG Data Security Standards is evidenced through:

- Policy compliance audits and spot checks
- Information Asset Registers and risk assessments
- Mandatory training completion records
- Incident and alert management systems
- Oversight by the Information Governance Working Group and Data Protection & Cyber Security Committee

Assurance Statement

Adherence to this policy provides assurance that Sherwood Forest Hospitals NHS Foundation Trust complies with the DSPT mandatory assertions and the National Data Guardian's Data Security Standards, and can evidence this compliance for DSPT submission, CQC inspection, internal audit and external assurance.

Appendix 3 Equality Impact Assessment (EIA) Form (Please complete all sections)

EIA Form Stage One:

Name EIA Assessor: J Plant		**Date of EIA completion:** 20th Feb 2026
Department: Medical Records		**Division:** CSTO
Name of service/policy/procedure being reviewed or created: Health Records Management Policy		
Name of person responsible for service/policy/procedure: J Plant		
Brief summary of policy, procedure or service being assessed: Policy regarding the management of paper and digital health records.		
Please state who this policy will affect: Patients or Service Users, Carers or families, Commissioned Services, Staff, Stakeholder organisations,		
Protected Characteristic	**Considering data and supporting information, could protected characteristic groups' face negative impact, barriers, or discrimination? For example, are there any known health inequality or access issues to consider? (Yes or No)**	**Provide a brief summary of what data or supporting information was considered to complete this assessment?**
Race and Ethnicity	No	Trust policy approach to availability of alternative versions Previous version of the policy
Sex	No	
Age	No	
Religion and Belief	No	
Disability	No	

Sexuality	No	
Pregnancy and Maternity	No	
Gender Reassignment	No	

Marriage and Civil Partnership	No No	
Socio-Economic Factors (i.e. living in a poorer neighbourhood / social deprivation)	No	

If you have answered 'yes' to any of the above, please complete Stage 2 of the EIA on Page 3 and 4.

What consultation with protected characteristic groups including patient groups have you carried out?
As far as you are aware are there any Human Rights issues be taken into account such as arising from surveys, questionnaires, comments, concerns, complaints or compliments?

On the basis of the information/evidence/consideration so far, do you believe that the policy / practice / service / other will have a positive or negative adverse impact on equality? (delete as appropriate)

EIA Form Stage Two:

Positive			Negative			
High	**Medium**	**Low**	**Nil**	**Low**	**Medium**	**High**

If you identified positive impact, please outline the details here:

N/A

Protected Characteristic	Please explain, using examples of evidence and data, what the impact of the Policy, Procedure or Service/Clinical Guideline will be on the protected characteristic group.	What is already in place in the policy or its implementation to address any inequalities or barriers to access including under representation at clinics, screening.	Please outline any further actions to be taken to address and mitigate or remove any in barriers that have been identified.
Race and Ethnicity	None	Alternative version could be created on request	N/A

Gender	None	N/A	N/A
Age	None	N/A	N/A
Religion	None	N/A	N/A
Disability	Visual accessibility of this document	End user has option to increase font size as required. Alternative version could be created on request	N/A
Sexuality	None	N/A	N/A
Pregnancy and Maternity	None	N/A	N/A
Gender Reassignment	None	N/A	N/A
Marriage and Civil Partnership	None	N/A	N/A
Socio-Economic Factors (i.e. living in a poorer neighbour hood / social deprivation)	None	N/A	N/A

Signature:
I can confirm I have read the Trust's Guidance document on Equality Impact Assessments prior to completing this form
Date:20/2/26