Solent
NHS Trust

Records Management & Information Lifecycle Management Policy for Clinical and Corporate Records

Solent NHS Trust policies can only be considered to be valid and up-to-date if viewed on the intranet. Please visit the intranet for the latest version.

Purpose of Agreement	This Policy is written to give the organisation a clear Information &Records Management Framework which includes advice and guidance on all aspects of Records Management and Data Quality to inform staff of their operational and legal responsibilities. This policy is not a stand-alone document and should be read in conjunction with the Records Management Code of Practice for Health and Social Care 2016
Document Type	☒ Policy □ SOP □ Guideline
Linked to O-SOP	IG03.1 Clinical Records Management for Gender Reassignment Patients O-SOP IG03.2 Electronic Recordings Conventions O-SOP
Reference Number	Solent NHST/Policy/IG/03
Version	5
Name of Approving Committees/Groups	Policy Steering Group, Clinical Executive Group
Operational Date	May 2022
Document Review Date	May 2025
Document Sponsor (Job Title)	Chief of Staff, and Interim Deputy Senior Information Risk Owner
Document Manager (Job Title)	Data Protection Officer and Head of Information Governance & Security
Document developed in consultation with	Policy Steering Group **Previous Versions:** Information Asset Owners Forum Information Asset Custodian Forum Information Governance Steering Group
Intranet Location	Business Zone > Policies, SOPs and Clinical Guidelines
Website Location	Policies and Procedures – Publication Scheme
Keywords (for website/intranet uploading)	Records; Records Management; Corporate Records; Clinical Records; Filing; Archiving; Shredding; Policy; IG03

Amendments Summary:

Amend No	Issued	Page	Subject	Action Date
			Update to reflect New organisation & SIRO change	March 2012
		35	Inclusion of Data Quality Guidance	March 2012
Version 3	January 2016	4 – 7 17 23 26 All	Executive Summary added Altering Electronic Record Entries added Unqualified Staff Entries – Process changed Restricting Access added RiO Lockdown process removed Removal of reference to a Local Records Procedure Removal of reference to Records Libraries	January 2016
Version 4	April 2019	All 25 27	Change reference from TPP to SystmOne, as this is the most commonly used name for this patient system Inclusion of the General Data Protection Regulations 2016 and Data Protection Act 2018 (replacing the Data Protection Act 1998) Change the naming of the adopted Records Management Code of Practice to "The Records Management Code of Practice for Health and Social Care 2016" Removal of Lord Chancellor's Department in agreement with sections 45(5) and 46(6) of the Act, as this has now been archived by the National Archives Addition to Transgender Patient Record Section Addition of the Logical Deleted Process	April 2019
Version 5	March 2022	Multiple	Removal of "Record Volume" and "Altering Records" from Section 6 – Now covered by the Clinical Records Standards Procedure. Removal of content from Section 7 – Now covered by the Clinical Records Standards Procedure. Removal of content from Section 8 – Now covered by the Records Management for Gender Reassignment Patients Procedure.	

			Removal of content from Section 11 – Now covered by the Electronic Records Management Procedure Removal of content from Section 13 – Now covered by the Data Quality Policy Removal of content from Section 14 – Now covered by the Missing or Lost Clinical Records Procedure Removal of Appendix A,B, C & D – as no longer applicable Appendix E, renamed Appendix A	

Review Log
Include details of when the document was last reviewed:

Version Number	Review Date	Name of Reviewer	Ratification Process	Notes
Prior to October 2010			Solent NHS Trust was established on 1st April 2010 through the integration of Southampton Community Healthcare (West) and Portsmouth Community & Mental Health Services (East). Solent NHS Trust is the Provider arm of NHS Southampton City.	Refer to; • NHS Southampton City's Records Management & Lifecycle Policy • NHS Southampton City's Standards of Clinical Records Policy • Portsmouth City's Records Management Policy
Version 2	November 2012	Sadie Bell, Information Governance Manager	Information Governance Steering Sub-Committee (Mar 13) NHSLA Policy Committee (Feb 13)	• Clinical Records section has been moved forward from section 7 to section 6 • Data Quality section has been moved forward from section 17 to section 10 • Transgender information expanded • Adopted Childrens Records • Protective Marking Review • RiO Lockdown Process added • General Review

Version 3	January 2016	Sadie Bell, Head of Information Governance	Policy Steering Committee	• See Amendments Summary
Version 4	April 2019	Sadie Bell, Data Protection Officer and Head of Information Governance & Security	Policy Steering Committee	• See Amendments Summary
Version 5	March 2022	Sadie Bell, Data Protection Officer and Head of Information Governance & Security	Policy Steering Committee, Clinical Executive Group	• See Amendments Summary Normal 3 year review

Contents

RECORDS MANAGEMENT & INFORMATION LIFECYCLE POLICY

1 Summary of Policy

1.1 All NHS records are public records (apart from the relevant exemptions under the Data Protection Legislation) under the terms of the Public Records Act 1958. Each member of staff is responsible for the records they create and use. Records Management is the process by which an organisation manages all the aspects of records whether internally or externally generated and in any format or media type, from their creation, all the way through their lifecycle to their eventual disposal.

1.1 This policy relates to all clinical and non-clinical (corporate) records held in any format by the Trust.

1.2 All NHS records are Public Records under the Public Records Acts. The Trust will take actions as necessary to comply with the legal and professional obligations set out in the Records Management: NHS Code of Practice

1.3 **Generic Records Management Standards for both Clinical and Corporate Records**

1.3.1 The standards incorporate national guidance and cover.

- Creation of Records
- Record Retention
- Archiving Records
- Retrieval and Access
- Transferring Records
- Record Volumes
- Altering Record Entries

1.4 **Security of Records**

1.4.1 All records should be held securely to prevent inappropriate/ unauthorised access and to protect the record from loss or accidental damage.

1.4.2 Staff using records must conform to the Data Protection principles and the requirements of the Caldicott report.

1.4.3 Security Standards for Electronic Records should observe the aforementioned guidance whilst also ensuring adherence to The Computer Misuse Act 1990. The relevance of the Act when used in application to electronic records is that it creates three offences of unlawfully gaining access to computer programmes.
The offences are:

- Unauthorised access to computer material;
- Unauthorised access with intent to commit or cause commission of further offences; and
- Unauthorised modification of computer material.

1.5 **Data Quality**

1.5.1 Should be managed and actioned in line with the organisations Data Quality Policy.

1.6 **Request for Records**

1.6.1 Any requests for records should be managed and actioned in line with the organisations Information Request Policy.

1.7 Missing or Lost Records – Reporting an Incident

1.7.1 Should be managed and actioned in line with the organisations Missing or Lost Clinical Records Procedure.

2 Introduction & Purpose

2.1 The policy recognises the need for an appropriate balance between openness and confidentiality in the management and use of electronic and paper records. The policy sets out the approach taken by the organisation in compliance with the Care Quality Commission, the Data Security & Protection Toolkit, The Freedom of Information Act 2000, and Data Protection Legislation.

2.2 Records Management is a discipline which utilises an administrative system to direct and control the Creation, Version control, Distribution, Filing, Retention, Tracking, 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.

2.3 The term 'Records Life Cycle' describes the life of a record from its creation/receipt through the period of its 'active' use, then into a period of 'inactive' retention (such as closed/discharged patient files which may still be referred to occasionally) and finally either confidential disposal or archival preservation.

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

2.5 All NHS records are public records (apart from the relevant exemptions under the Data Protection Legislation) under the terms of the Public Records Act 1958. Each member of staff is responsible for the records they create and use. Records Management is the process by which an organisation manages all the aspects of records whether internally or externally generated and in any format or media type, from their creation, all the way through their lifecycle to their eventual disposal.

2.6 The Records Management Code of Practice for Health and Social Care 2016. This document sets out a schedule for the minimum retention periods for many types of records and is based on current legal requirements and potential best practice. This policy adopts the retention and review guidance within that document.

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

2.7 The Board has adopted this records management policy and is committed to ongoing improvement of its records management functions as it believes that it will several organisational benefits from so doing. These include:

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

2.8 The organisation believes that its internal management processes will be improved by the greater availability of information that will accrue by the recognition of records management as a designated corporate function.

2.9 This document sets out a framework within which the staff responsible for managing the organisation's records can develop specific policies and procedures to ensure that records are managed and controlled effectively, and at best value, commensurate with legal, operational and information needs.

3 Scope & Definitions

3.1 This policy applies to locum, permanent, and fixed term contract employees (including apprentices) who hold a contract of employment or engagement with the Trust, and secondees (including students), volunteers (including Associate Hospital Managers and Patient Safety Partners), bank staff, Non-Executive Directors and those undertaking research working within Solent NHS Trust, in line with Solent NHS Trust's Equality, Diversity and Human Rights Policy. It also applies to external contractors, agency workers, and other workers who are assigned to Solent NHS

3.2 Solent NHS Trust is committed to the principles of Equality and Diversity and will strive to eliminate unlawful discrimination in all its forms. We will strive towards demonstrating fairness and Equal Opportunities for users of services, carers, the wider community, and our staff.

3.3 This policy relates to all clinical and non-clinical records held in any format by the Trust. These include:

- All records whether electronic or paper (e.g. personnel, estates, financial and accounting records, notes associated with complaints),
- Health records (for all specialties and including private patients, including x-ray and imaging reports, registers, etc.)

3.4 This policy is not intended for retrospective application to existing notes, no longer in use.

3.5 **Abbreviations**

CQC	Care Quality Commissioner
HCP	Health Care Professional
IAC	Information Asset Custodian
IAO	Information Asset Owner
PAS	Patient Administration System
PID	Personally Identifiable Data
PMI	Patient Master Index
SCR	Summary Care Registration

SIRO	Senior Information Risk Officer
SIRI	Serious Incident Requiring Investigation

3.6 Definitions

A Document - provides guidance and/or direction for performing work, making decisions, or rendering judgments which affect the quality of the products or services that customers receive. A *document* should be construed to mean any physical guide or direction whether written, video tape, physical sample, sample drawing, computer program or otherwise.

A Record - proves that some type of required quality system action took place. Sometimes documents become records. For instance, Management Review Minutes become the record that a Management Review has taken place.

- Records are available when needed - from which the organisation can form a reconstruction of activities or events that have taken place.
- Records can be accessed - records and the information within them can be located and displayed in a way consistent with its initial use, and that the current version is identified where multiple versions exist.
- Records can be interpreted - the context of the record can be interpreted: who created or added to the record and when, during which business process, and how the record is related to other records.
- Records can be trusted – the record reliably represents the information that was used in, or created by, the business process, and its integrity and authenticity can be demonstrated.
- Records can be maintained through time – the qualities of availability, accessibility, interpretation, and trustworthiness can be maintained for as long as the record is needed, perhaps permanently, despite changes of format.
- Records are secure - from unauthorised or inadvertent alteration or erasure, that access and disclosure are properly controlled, and audit trails will track all use and changes. To ensure that records are held in a robust format which remains readable for as long as records are required.
- Records are retained and disposed of appropriately in compliance with The Records Management Code of Practice for Health and Social Care 2016 which has been adopted by Solent NHS Trust for consistent retention and disposal procedures, which include provision for appraisal and the permanent preservation of records with archival value.
- The organisation has an off-site records storage contractor with whom records are securely stored.
- The Information Governance Team hold a list of all records stored in off-site storage and they hold a record of authorised users who are permitted to retrieve records from off-site storage. They also maintain a record of all records that have been sent for destruction and the related destruction certificates.
- Staff are trained - so that all staff are made aware of their responsibilities for record-keeping and record management.

A “missing” record is a record that either cannot be found or is unavailable when required.

A “lost” record is a record that after substantial searches, by more than one individual, cannot be located.

Weeding/Decanting – this is the process by which records are selected as inactive (not current) and transferred either to an inactive records storage area on site (space permitting) or to off-site storage with an organisational approved contractor. It is best practice that this exercise is conducted annually or where patient turnover is high, more regularly.

4 Legal and Professional Obligations

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

- The Public Records Act 1958
- The Data Protection Act 2018
- UK General Data Protection Regulations 2021
- The Freedom of Information Act 2000
- The Common Law Duty of Confidentiality; and
- The Records Management Code of Practice for Health and Social Care 2021
- The NHS Confidentiality Code of Practice.
- Lord Chancellors Code of Practice for Records Management

Any new legislation affecting records management as it arises

5 Generic Records Management Standards for both Clinical and Corporate Records

The standards incorporate national guidance such as the Data Security & Protection Toolkit and the Care Quality Commission.

It is recognised that within multidisciplinary teams e.g. Intermediate care teams, there may be organisational differences to implementing some of these standards. If that is the case, service managers must liaise with the Information Governance Team to ensure that any risk is minimised.

Professional groups should also take into account their own regulatory body standards, e.g. Nursing and Midwifery Council.

5.1 Information/Record Systems

All system (manual and electronic) changes or new systems must be authorised by senior management of the organisation in consultation with the IT services provider. They must be checked to ensure they comply with data protection requirements and approved by the Information Governance Team, who will undertake a Data Protection Impact Assessment in line with the Trust's Data Protection By Design Procedure.

5.2 Creation of Records

All services should have in place a process for documenting its activities in respect of records management. This process should take into account the legislative and regulatory environment in which the unit operates. All records should be complete and accurate, to facilitate an audit or examination of the organisation, its patients, staff and others affected by its actions, and provide authentication of the records so that evidence derived from them is shown as credible and authoritative.

Registration of a created record is the act of giving the record a unique identifier upon creation and addition to a record keeping system.

All record documentation is to be bound and secured in a logical sequence within the record folder in accordance with local processes, this demonstrates the order and chronology of care.

Records created should be arranged in a record keeping system that enables quick and easily retrievable information.

Once a record is created, it will need to be accessed, updated, and may need to be disclosed but must also be protected. Where the record is a duplicate or partially holds information held elsewhere, it must be possible to keep the record accurate and up to date with the master record. It is worth considering whether the information you wish to record could be added to a central record already in place to avoid these issues and facilitate improved records management within the organisation.

This issue is particularly important when considering the creation of a patient health record. Some specialities have taken the decision that a separate health record held within their service provides higher quality care to the patient. This decision needs to be strictly justified and regularly reviewed with consideration given to developments such as the National Care Record Service and CQC.

5.3 Filing of Records

Record filing instructions must be produced for all electronic and paper-based records. Processes must provide.

- A clear and logical filing structure that aids retrieval of records. Ideally, the filing structure should reflect the way in which corporate records are filed to ensure consistency. However, if it is not possible to do this, the names allocated to files and folders should allow intuitive filing.
- The agreed filing structure should also help with the management of the retention and disposal of records
- A referencing system should be used that meets the organisation’s business needs and can be easily understood by staff members that create documents and records. Several types of referencing can be used, for example, alphanumeric; alphabetical; numeric; keyword.
- It may be more feasible in some circumstances to give a unique reference to the file or folder in which the record is kept and identify the record by reference to date and format.

5.4 Record Retention

It is a fundamental requirement that all records are retained for a minimum period for legal, operational, research and safety reasons.

All staff that may create or add entries to records must to be aware of and follow The Records Management Code of Practice for Health and Social Care 2016 that has been adopted by Solent NHS Trust in relation to the Retention and Disposal of all Records. Staff need to be aware of the differing retention periods that exist e.g. patients involved with clinical trials will need to have their records kept for a longer period.

To ensure that legal and statutory requirements are met, with regards to the retention periods of records, the Information Governance Team should be notified of any new types of records that do not appear on The Records Management Code of Practice for Health and Social Care 2021, so that a lifecycle for the record is determined at the point of creation.

5.5 Destroying or Restating Records Outside of Retention Periods

Where a service feels that there is a need to retain a record longer than its retention period or destroy a record prior to a retention period e.g. destroying a video of a group clinical session after a year, then this must be risk assessed and then approved by the Trust's Head of Information Governance, Senior Information Risk Owner (SIRO) and Caldicott Guardian.

5.6 Disposal of Records

Records will be destroyed under confidential conditions; please refer to the Data Protection Compliance Policy for further information.

5.7 Archiving Records

Where there is a need to archive, as well as weeding and decanting, services should register an authorised member of staff who will be responsible for the archiving and retrieval of the records, with the Information Governance Team. When completed, services will then need to place records into approved storage boxes (do not mix records where destruction date is different).

Archived records should also be catalogued using the online archiving system and have an identified retention date.

No decision to store records at an alternative off-site storage, other than then approved contractor, should be made by services without prior consultation with the Information Governance Team, who where applicable will seek advice from the SIRO and Caldicott Guardian.

Where electronic records are stored there should be an archive facility on the server or a suitable media available e.g. cd stored in a logical file structure to ensure safe preservation for future resurrection). This will be overseen by the Information Governance Team.

Archives – Records identified more appropriately as archives should be offered to the national archives, which will make a decision regarding their long-term preservation.

5.8 Retrieval and Access

Access to all records must be restricted to authorised personnel wherever they are stored, and records must be securely locked away.

If a service provides 24-hour care and admits patients over the 24-hour period, then records must be able to be retrieved at any time, seven days a week and documented procedures in place.

For additional information on patient held records please see section 7.9 of this policy

5.9 Transferring Records

Movement of any records (even on the same site), should always be logged in inventory format, either on an approved records tracer, a register book, or an electronic system such as SystmOne. A risk assessment form should be completed prior to relocation.

Please refer to the Trust's Data Protection Compliance Policy for further information on the transferring of Personally Identifiable Data (PID).

5.10 Protective marking

The HMG Security Policy Framework describes the, "principles and approaches that the UK Government applies to protect its assets" and it focuses on security outcomes that it considers necessary to achieve its aim of, "a proportionate and risk managed approach to security that enables government business to function effectively, safely and securely."

The Policy Framework advises that the considerations it specifies are mandatory for all Departments and Agencies and that there are minimum levels to be achieved which may in turn assist in compliance with a range of statutory requirements, including the Data Protection Legislation. It further specifies that organisations including the NHS and shared services must protect material in the appropriate way.

The Policy Framework is clear that information should be assigned a value according to a predetermined list of definitions and then clearly marked in accordance with those definitions. The definitions currently are comprised of five markings: Top Secret, Secret, Confidential, Restricted and Protect). The definitions indicate; "in descending order the likely impact resulting from compromise or loss."

Material which is unmarked for security purposes is "unclassified". In these circumstances, the Framework Policy states that, "the term "Unclassified" or "Not Protectively Marked" may be used to indicate positively that a protective marking is not needed."

For further information on protective marking, please refer to The HMG Security Policy Framework https://www.gov.uk/government/publications/security-policy-framework

6 Clinical/Health Records

A Health Record is defined as:

- consists of any information relating to the physical or mental health or condition of an individual or about the care they receive is recorded and stored in a health and care record.'

- has been made by or on behalf of a health professional in connection with the care of that individual' checked and correct.

Any clinical records used by the Solent NHS Trust staff, which is owned/originated from another organisation i.e. Hospitals, Social Services, Education etc. must be managed in accordance with this policy and the Trust's Clinical Records Management Standards Procedure (please see procedure for further information on the management of clinical / health records).

6.1 **Restricting Access**

Access to both paper-based and electronic records should be restricted to service/organisational level. If a patient requests for information to be restricted further, arrangements should be made locally and organisationally to ensure that this is actioned. Further advice on how to undertake this can be obtained from the Information Governance Team and where applicable System Processed (e.g. SystmOne). Information should only be accessed by a third-party organisation with patient consent and if an Information Sharing Agreement is in place.

6.2 **Notification of a death**

When notification of a death is received, the records should be updated accordingly. Health Records must be stamped 'Deceased' on the right-hand side of the front cover and annotated with the date of death. Future appointments and/or patient transport arrangements should be cancelled. Electronic systems must be updated accordingly. The health record should be returned to the appropriate store, where arrangements will be made for archiving in accordance with the organisational retention and disposal schedule.

7 Clinical Records Management for Gender Reassignment Patients

Summary: In summary the Trust's position is as follows –

- Only persons who have "protected characteristics of gender reassignment" are explicitly protected under the Equality Act 2010.

- The Equality Act states that a person has a protected characteristic of gender reassignment if the individual is to undergo, is undergoing, or has undergone a process (does not have to be a medical process / procedure) for the purpose of reassigning their sex by changing physiological or other attributes of sex.

- The Human Rights Act also offers protection to individuals (whether that individual has obtained formal legal recognition in their acquired gender by being issued with a GRC).

- An individual can obtain formal legal recognition of their acquired gender under the Gender Recognition Act 2004; but are not compelled to do so.

- Names and titles on medical records can be changed at the point that the individual changes their gender role permanently (or sooner if this is requested and there is some evidence of the intended permanency) such that the individual has a protected characteristic of gender reassignment in line with the Equality Act.

- Consequently, prior to obtaining a GRC, if an individual can show that they fall within (2) above, then the Trust should be changing an individual's name and title on their electronic or paper folder. This ties in with NHS Guidance which says "names and titles must be changed to reflect current gender status. This can be done as a matter of courtesy and is not dependent on having a GRC". Of course, this should be discussed with the patient before being implemented.

- Although there is no obligation to change the individual's historical notes contained in the file (as this could potentially put health at risk); it may be sensible to ensure historical information has limited access (confined to medical professionals) so that it is not accessed by administrative or reception staff.

- NHS Guidance also suggests that letters and envelopes should be addressed in accordance with the individual's new gender role (unless they have requested otherwise).

- Where a GRC has been obtained, the protection of historical gender information is sacrosanct, and may be subject to criminal sanction if breached unless it falls within limited exemptions.

  Please refer to the Trust's Clinical Records Management for Gender Reassignment Patients Procedure for further information on the management of such clinical / health records

8 Clinical Records Management for Adopted Children

8.1 Under adoption legislation, an adopted child is given a new NHS number, and all previous medical information relating to that child is put into a newly created health record (the old records must be retained / archived until the child's 75th birthday). Any information relating to the identity or whereabouts of the birth parents should not be included in the new record. The change of name, NHS number and transfer of previous health information into a new health record should take place for all records. There should not then be any difficulty in obtaining information about the child's previous treatment.

Whilst changing or omitting information from medical records would usually be contrary to ethical and professional guidance this is not the case for the records of adopted children as there is a legal requirement that it takes place.

The pre-adoptive information should be regarded as confidential and the service must ensure that robust systems are in place for access or disclosure.

For further information on how this process works, please refer to section 10 of this policy, which explains how an old record is closed and new record is opened.

9 Logically Deleted Process

9.1 When a patient applies for a new NHS Number, whether that be a result of "change in identity" or adoption, their old NHS Number is considered to be "logically deleted", this in effect means, no longer applicable nor accessible.

Weekly the Information System Team will receive a report of “logically deleted” NHS Numbers and will perform an exercise to remove these patients records from the electronic patient systems.

If the patient has an open referral to a service, the Information Systems Team will identify the patients New NHS Number and notify an identified key link with the service the patient is being seen by, of the following.

- The fact that the patient’s old record has been “logically deleted”
- The patients New NHS Number
- Dates of planned appointments, so these can be booked again under the New NHS Number
- Requesting that a relevant Health Care Professional is identified to review the old record and copy over any clinically pertinent information into the new record.

Once a relevant Health Care Professional has been identified, the Information Systems Team will provide them with temporary access to the “logically deleted” record, so that they can transfer any clinically pertinent information into the new record. The process around this differs slightly, depending on the reason for the “logical deletion” and staff should refer to Sections 8 or 9 of this policy, depending on the reason a new record has been created.

You cannot merge the records nor copy over a complete set of the “logically deleted” record.

10 Effective Corporate Records Management

10.1 Each department within the organisation shall keep adequate records to document its activities.

Corporate record keeping systems shall classify and group records according to business functionality.

Wherever possible, records which have been created electronically shall be captured and stored in electronic records keeping systems i.e. not printed and stored in paper form, electronic records will be managed like any other record in accordance with this policy.

Records where appropriate should be captured and stored within designated folders and stored in shared folders.

Please refer to the Electronic Records Management Procedure for further details.

11 Security of Records

11.1 All records should be held securely to prevent inappropriate/ unauthorised access and to protect the record from loss or accidental damage.

11.2 Staff using records must conform to the Data Protection principles and the requirements of the Caldicott report. This includes recognising confidentiality as an obligation, recording information accurately and consistently and keeping information private and physically/ electronically secure. This also includes ensuring records are only accessed by staff, for work related reasons. Failure to do so is a breach of both policy and law and could lead to HR Disciplinary Processes and possible Prosecution and Fines. Further detailed information can be found in the Data Protection Compliance Policy. The NHS Confidentiality Code of Practice also gives practical guidance on security of patient information.

11.3 Records containing personal identifiable or sensitive information are confidential documents protected by Data Protection Legislation and the NHS Confidentiality Code of Practice. The records should be kept in a secure place (either where they are under constant observation or in a locked cabinet or room) both when in use and when in storage.

11.4 Access to storage facilities must be limited to designated staff

11.5 Records which must be kept in a professional's possession (e.g. overnight) are to be afforded the same security as those stored in the office, i.e. out of sight in a locked facility and for the minimum amount of time possible.

11.6 Security Standards for Electronic Records should observe the guidance whilst also ensuring adherence to The Computer Misuse Act 1990. The relevance of the Act when used in application to electronic records is that it creates three offences of unlawfully gaining access to computer programmes.

The offences are:

- Unauthorised access to computer material
- Unauthorised access with intent to commit or cause commission of further offences; and
- Unauthorised modification of computer material.

Access is defined in the Act as

- Altering or erasing the computer program or data
- Copying or moving the program or data
- Using the program or data; or
- Outputting the program or data from the computer in which it is held (whether by having it displayed or in any other manner).

Unlawful access is committed if the individual intentionally gains access; knowing they are not entitled to do so; and is aware they do not have consent to gain access, even if they have access to the record / system.

The 'further offence' applies if unauthorised access is carried out with intent to commit or cause an offence.

The 'Modification' offence applies where an individual does any act causing unlawful modification of computer material and does so in the knowledge that such modification is unlawful, and with the intent to:

- Impair the operation of any computer

- Prevent or hinder access to any program or data held in any computer; or
- Impair the operation of any such program or the reliability of any such data.

Passwords must never be shared.

Suspected fraud, bribery and/or Corruption in respect unlawful data access, removal and/or use should be reported to the Trusts Local Counter Fraud Specialist in accordance with the Local Fraud, Bribery and Corruption Policy and NHS Counter Fraud Manual.

12 Data Quality

12.1 For further information refer to the Trust's Data Quality Policy

13 Request for Records

13.1 Any requests for records should be managed and actioned in line with the organisations Information Request Policy.

14 Missing or Lost Records – Reporting an Incident

14.1 Please refer to the "Missing or Lost Clinical Records Procedure"

15 Roles and Responsibilities

The responsibility for local records management is devolved to the relevant Directors, Directorate Managers, Service Managers, Heads of Departments and Information Asset Custodians, other units and business functions within the Trust have overall responsibility for the management of records generated by their activities, i.e. for ensuring that records controlled within their unit are managed in a way which meets the aims of the Trust's records management policies. They are responsible for examining the records of their service area to determine the compliance of the standards contained within this document to ensure that a co-ordinated approach to the management of the record is maintained.

15.1 **Chief Executive**
The Chief Executive has overall responsibility for records management in the Organisation. The accountable officer is responsible for the management of the organisation and for ensuring appropriate mechanisms are in place to support service delivery and continuity. Records management is key to this as it will ensure appropriate, accurate information is available as required.

The Chief Executive has a particular responsibility for ensuring that the organisation corporately meets its legal responsibilities, and for the adoption of internal and external governance requirements.

15.2 **Caldicott Guardian and Senior Information Risk Officers (SIRO)**
The Organisation's Caldicott Guardian and SIRO have a particular responsibility for reflecting patients' interests regarding the use of patient identifiable information. They are responsible for ensuring patient identifiable information is shared in an

appropriate and secure manner.

15.3 **Information Asset Owners**

The Information Asset Owner (IAO) is a senior member of staff who is the owner for one or more identified information assets of the organisation.

There are several IAOs within the organisation, whose departmental roles may differ. IAOs will work closely with other IAOs of the organisation to ensure there is comprehensive asset ownership and clear understanding of responsibilities and accountabilities. IAOs will support the organisation's SIRO in their overall information risk management function as defined in the organisation's policy.

15.4 **Information Governance Team**

The Information Governance Team is responsible for the overall development and maintenance of records management practices throughout the organisation, in particular for drawing up guidance for good records management practice and promoting compliance with this policy in such a way as to ensure the easy, appropriate and timely retrieval of patient information.

15.5 **Service Managers and Local Records Manager (Information Asset Custodians (IAC)**

Service Managers and Local Records Managers (IAC's) are responsible for ensuring that this policy is implemented, and that the records management system and processes are developed, co-ordinated and monitored.

All Service managers and Local Records Managers are responsible for examining the records of their service area and to ensure there is structure and processes in place to meet compliance of the standards contained within this document.

All Service managers are responsible for liaising with appropriate departments to ensure that a co-ordinated approach to the management of the record is maintained.

All Service managers and Local Records Managers are responsible for and must participate in the annual clinical audit which forms part of the Information Governance standards requirements.

Service Managers and Local Records Managers must ensure that all grades of clinical staff receive regular training on clinical record keeping.

15.6 **All Staff**

All staff under the Public Records Act, whether clinical or administrative, who create, receive, and use records have records management responsibilities. All staff must ensure that they keep appropriate records of their work and manage those records in keeping with this policy and with any guidance subsequently produced.

All users of Healthcare Records must be aware of their legal obligations and abide by the requirements of Data Protection Legislation and Principles of Caldicott.

All users of Healthcare Records must be aware of the process for managing Freedom of Information requests and act on it as required.

Each member of staff is responsible for the records they create and use.

16 Failure to Comply with the Policy

16.1 If a service feels it cannot comply with all or part of an IG policy/ procedure, they have a duty to undertake a risk assessment which will be approved by the services Information Asset Owner and Information Governance Team. Failure to do so could result in disciplinary action. For further advice services should contact the Information Governance Team.

Failure to comply with this policy will initiate the Improving and Managing Conduct Policy (unless agreed exceptions have been approved).

17 Training

17.1 All staff will be made aware of their responsibilities for record-keeping and record management.

All Trust staff will be made aware of their responsibilities regards Data Protection, through their annual Information Governance Training.

It is the responsibility of the Information Governance Team to produce the training tool

Compliance with this training requirement will be monitored by the Learning & Development Team in conjunction with the Information Governance Team via a reporting mechanism learning and development training tool.

18 Equality & Diversity and Mental Capacity Act

18.1 A thorough and systematic assessment of this policy has been undertaken in accordance with the Trust’s Policy on Equality and Human Rights.

The assessment found that the implementation of and compliance with this policy has no impact on any Trust employee on the grounds of age, disability, gender, race, faith, or sexual orientation. See Appendix A

19 Success Criteria/Monitoring the Effectiveness of the Policy

19.1 The monitoring of this policy and its effectiveness and maintenance will be audited annually using the Data Security & Protection Toolkit (DSPT) for PCTs or sooner if new legislation, codes of practice or national standards are introduced. The DSPT audit is a self-assessment audit undertaken by the Information Governance Team; additionally, the submission is audited annually by external auditors, South Coast Audits.

The owner/author of the policy is responsible for undertaking this audit and ensuring the policy's effectiveness.

The Information Governance Team will on a weekly basis review and monitor all Information Governance and Records Management incidents and where required conduct full investigations.

20 Review

20.1 This document may be reviewed at any time at the request of either at staff side or management, but will automatically be reviewed three years from initial approval and thereafter every three yearsunless organisational changes, legislation, guidance or non-compliance prompt an earlier review

21 Reference and Links to Other Documents

This policy must be read in conjunction with the policies below that are available on the Intranet

21.1 **Policies:**

- Information Request Policy
- Data Protection Compliance Policy
- Registration Authority Policy
- Data Quality Policy

21.2 **Procedures:**

- Registration Authority Procedure
- Clinical Records Standards Procedure
- Clinical Records Management for Gender Reassignment Patients Procedure
- Electronic Records Management Procedure
- Missing or Lost Clinical Records Procedure
- Data Protection by Design Procedure

21.3 **Code of Practices:**

- Destruction of Confidential Waste
- The Records Management Code of Practice for Health and Social Care 2021

Appendix A – Equality Impact Assessment

Step 1: Scoping and Identifying the Aims

Service Line / Department	Information Governance	
Title of Change:	Records Management & Information Lifecycle Policy	
What are you completing this EIA for? (Please select):	Policy	*(If other please specify here)*
What are the main aims / objectives of the changes	To ensure that staff have a clear and structured policy, directing on the management of the Trust's information and records	

Step 2: Assessing the Impact

Please use the drop-down feature to detail any positive or negative impacts of this document /policy on patients in the drop-down box below. If there is no impact, please select "not applicable":

Protected Characteristic	Positive Impact(s)	Negative Impact(s)	Not applicable	Action to address negative impact: *(e.g. adjustment to the policy)*
Sex			x	
Gender reassignment			x	
Disability			X	
Age			X	
Sexual Orientation			X	
Pregnancy and maternity			X	
Marriage and civil partnership			X	
Religion or belief			X	
Race			x	

If you answer yes to any of the following, you MUST complete the evidence column explaining what information you have considered which has led you to reach this decision.

Assessment Questions	Yes / No	Please document evidence / any mitigations
In consideration of your document development, did you consult with others, for example, external organisations, service users, carers or other voluntary sector groups?)	Please select	
Have you taken into consideration any regulations, professional standards?	Please select	

Step 3: Review, Risk and Action Plans

How would you rate the overall level of impact / risk to the organisation if no action taken?	Low	Medium	High
	■	□	□
What action needs to be taken to reduce or eliminate the negative impact?	N/A		
Who will be responsible for monitoring and regular review of the document / policy?	Data Protection Officer		

Step 4: Authorisation and sign off

I am satisfied that all available evidence has been accurately assessed for any potential impact on patients and groups with protected characteristics in the scope of this project / change / policy / procedure / practice / activity. Mitigation, where appropriate has been identified and dealt with accordingly.

Equality Assessor:	*Sadie Bell*	*Date:*	*09/05/2022*