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	[x] Policy [ ] SOP [ ] Guideline
Reference Number	Solent NHST/Policy/IG/03
Version	3
Name of Approving Committees/Groups	Policy Steering Group
Operational Date	May 2019
Document Review Date	May 2022
Document Sponsor (Name & Job Title)	David Noyes, Chief Operating Officer and Senior Information Risk Owner
Document Manager (Name & Job Title)	Sadie Bell, 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	Policies and Procedures – Solent
Website Location	Policies and Procedures – Publication Scheme
Keywords (for website/intranet uploading)	Records; Records Management; Corporate Records; Clinical Records; Filing; Archiving; Shredding

Amendments Summary:

Amend No	Issued	Page	Subject	Action Date
1			Update to reflect New organisation & SIRO change	March 2012
		35	Inclusion of Data Quality Guidance	March 2012
2	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
3	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 be archived by the National Archives Addition to Transgender Patient Record Section Addition of the Logical Deleted Process	April 2019

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

Contents

1 Executive Summary

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.

1.2 This policy relates to all clinical and non-clinical records held in any format by the Trust.

1.3 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

1.4 Generic Records Management Standards for both Clinical and Corporate Records

1.4.1 The standards incorporate national guidance and cover;

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

1.5 Clinical/Health Records

1.5.1 **Primary Records:** Services within Solent NHS Trust have mostly transferred the management of records from a paper based system to an electronic system e.g. SystmOne

1.5.2 **NHS Numbers:** As of September 2009 it was mandated that NHS numbers must be recorded on all active patient records and for all communication in relation to patient care.

1.5.3 **Completeness of Clinical Records:** Part of the multi-disciplinary care process should be to audit the quality of clinical information on which decisions about the care of the patient are made. This should include a review of**;**

- Care Plan's
- Decisions Made
- Care Delivery
- Information Shared

1.5.4 **Logging Queries:** Process should be in place to log and record queries made either by patients or internal sources, with regards to the content of medical records.

1.5.5 **Unregistered or Registered Staff:** All entries made by an unregistered member of staff, must be countersigned, until they have been assessed as competent.

1.5.6 **Verbal Communication:** All verbal communication about patients care, treatment and support must be documented within the patient's record.

1.5.7 **Patient Held Records:** Patient held Records are defined as health records which are kept within the home of the patient or family. A covering letter should be placed at the front of each patient held record.

1.5.8 **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.

1.5.9 **Notification of a death:** When notification of a death is received, the records should be updated accordingly.

1.5.10 **Clinical Records Management for Gender Reassignment Patients:** Refer to Section 8 of this Policy for information on records management for gender reassignment patients.

1.5.11 **Clinical Records Management for Adopted Children:** 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). Refer to Section 9 this Policy for further information.

1.6 Effective Corporate Records Management

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

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

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

1.6.4 **Naming Folders, Files and Documents:** Naming conventions are standard rules to be used for both naming documents and electronic folders and are designed to make it easier to find documents.

1.6.5 **Corporate Standards for Ownership of Documents:** All records that are produced must adhere to the corporate standards for records. Refer to section 11 of this Policy for further details, including Naming Convention Principles.

1.7 Security of Records

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

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

1.7.3 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.

1.8 Record Tracking Procedures

1.8.1 All records movements will be tracked, either in paper format of electronically on the patient system (where this is used by the service).

1.9 Data Quality

1.9.1 The Trust, service users and the public must have confidence in the quality of data used for the provision of patient care, information governance, management and planning, commissioning and accountability. For further information staff should refer to the Trust's Data Quality Policy.

1.10 Request for Records

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

1.11 Missing or Lost Records – Reporting an Incident

1.11.1 **Procedure for Records that cannot be found – unavailable / loss:** The member of staff who identified the record as missing should report the unavailable / loss record (this applies to records containing Personally Identifiable Data or Sensitive Data) to their supervisor/Line manager, work colleagues and Information Asset Custodian as soon as possible. Further details can be found in Section 16.2 of this policy.

1.11.2 If the record can not be located the event must be entered using the Electronic Incident reporting system, which will notify the Information Governance Team.

1.12 Unavailable clinical records

1.12.1 A record is regarded as unavailable if it is in use elsewhere and/or cannot be retrieved in time for an appointment or within 24 hours of admission. The record is considered missing. A temporary record should be created.

1.13 Breaches to Confidentiality

1.13.1 A record containing personally identifiable or sensitive data must be kept secure at all times and access restricted to appropriate and authorised personal. Any breaches or potential breaches of confidentiality must be reported using an the online incident reporting system.

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 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.

2.3 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.

2.4 The Records Management Code of Practice for Health and Social Care 2016. Appendix 3 of 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.

2.5 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.

2.6 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 gain a number of 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

2.7 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.

2.8 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), bank, volunteers (including Associate Hospital Managers), Non-Executive Directors, governors 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 Trust.

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 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.

3.5 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.

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

Definitions

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

4 Aims of our Documents and Records Management System

4.1 The aims of our Records Management System are to ensure that staff understand the difference between a document and a record

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 is able to form a reconstruction of activities or events that have taken place.
- Records can be accessed - records and the information within them can be located and displayed in a way consistent with its initial use, and that the current version is identified where multiple versions exist.
- Records can be interpreted - the context of the record can be interpreted: who created or added to the record and when, during which business process, and how the record is related to other records.
- Records can be trusted – the record reliably represents the information that was actually used in, or created by, the business process, and its integrity and authenticity can be demonstrated.
- Records can be maintained through time – the qualities of availability, accessibility, interpretation and 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 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.

5 Legal and Professional Obligations

5.1 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;
- The General Data Protection Regulations 2016;
- The Freedom of Information Act 2000;
- The Common Law Duty of Confidentiality; and

- The Records Management Code of Practice for Health and Social Care 2016
- The NHS Confidentiality Code of Practice.
- Lord Chancellors Code of Practice for Records Management

Any new legislation affecting records management as it arises

6 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 and local records 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.

All services via their local records manager (Information Asset Custodian) must compile and implement a service specific Local Record Procedure outlining how the service and its staff comply with the Record Management Standards, stated within this policy.

6.1 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 Compliance Policy.

6.2 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.

6.3 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.

6.4 Record Retention

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

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. In particular 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 of time.

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 2016, so that a lifecycle for the record is determined at the point of creation.

Destroying or Retaining Records Outside of Retention Period

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.

For a form to be completed for approval refer to Appendix A.

6.5 Disposal of Records

Records will be destroyed under confidential conditions using an approved contractor and a

certificate of destruction will be stored centrally by the Information Governance Team, along with a locally stored Spreadsheet relevant to records destroyed.

6.6 Archiving Records

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.

Where there is a need to archive 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) and complete two registration forms, Appendix B. One is to be placed inside the storage box and one placed on the outside of the storage boxes. Records will not be archived without this form being completed.

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.

6.7 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

6.8 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.

If physically transporting personally identifiable data (PID) or confidential records then ensure that you carry them or store them out of view (e.g. boot of your car),and **always** in a locked lockable bag and that they are returned to the service area as soon as possible. When

in procession of staff member PID should be offered the same level of security, as it would be in an office / clinic environment. Staff should risk assess, how best to secure this information, in accordance with policy. Personally identifiable data (PID) or confidential records must never be left in a car overnight.

All records that leave the organisations premises must be logged for security audit purposes and in accordance with the Data Protection Compliance Policy.

All transfers of data containing personally identifiable or sensitive data, whether via email, post or telephone must be in accordance with the Data Protection Compliance Policy. Please also refer to section 12 of this policy for additional information on ensuring the security of records.

6.9 Record Volumes (Paper Records)

The volume number should be clearly visible on the records front cover or within the electronic documents name.

Volumes of records (where applicable that have become too large (approx 5 centimetres/ 2inches in width or that exceed 1 kilo/2.2llbs,) need to be closed and a new volume created.

Clinical records, where applicable, must be recorded on electronic systems such as SystmOne, PAS, etc… Where this is not possible labels for the new volumes of records should be printed, the label will indicate if this is volume 1 of 2 or volume 2 of 2.

Alternatively if the record is not on SystmOne, PAS, etc… a new record cover must be created identifying the volume number and date the volume was opened.

The previous volume must state the data of closure on the front cover and archived.

Closure - Records should be closed (i.e. made inactive and transferred to secondary secure or off site storage) as soon as they have ceased to be in active use other than for reference purposes, including closure of a volume. An indication that a file of paper records or folder of electronic records has been closed, together with the date of closure, should be shown on the record the front cover or within the electronic record as well as noted in the index or database of the files/folders. Where possible, information on the intended disposal of electronic records should be included in the metadata when the record is created.

Closed records that are reinstated must be tracked using the agreed system in place and returned to storage areas on site or to authorised off-site facilities. This activity must be noted in the index or database of the files/folders.

The storage of closed records should follow accepted standards relating to environment, security and physical organisation of the files.

6.10 Altering Record Entries

Paper: Simple alterations are made by scoring out with a single line followed by the correct entry, with date, time and signature and designation, and must be countersigned by a registered member of staff. Correction fluid must not be used. If any point is later found to be inaccurate, misleading or misreported, a separate note should be made to this effect. Electronic records have a built in audit trail to undertake this task.

Electronic: Any information or document(s) that are uploaded or marked on a patient record in error should be reported as an incident and Trust processes should be followed in order for the record to be marked in error.

6.11 Electronic Records

Electronic record systems must adhere to the same records management procedures as paper records.

6.12 Scanning Records

For reasons of business efficiency or in order to address problems with storage space, services may consider the option of scanning into electronic format, records which exist in paper format.

When scanning, digitising and then storing records electronically, consider legal admissibility by adopting the procedures recommended in the BSI publication 'BIP 0008:2004 Code of practice for legal admissibility and evidential weight of information stored electronically'

Services selecting the option to scan documents should also identify all records vital to the continuing functioning of the activities of the Trust in the event of business continuity arrangements and make provision for their protection.

No decision to scan should be made by services without first having discussed with the Information Governance Team, who where applicable will seek advice from the SIRO and Caldicott Guardian.

6.13 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 considered to be, "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

7 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'
- 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 their Records Policy.

7.1 Primary Records

Services within Solent NHS Trust have transferred the management of records from a paper based system to an electronic system e.g. SystmOne, R4, Inform, etc…

Where services have moved over to electronic record management systems and summary of key information and scanned copies of important documents must be transferred/copied over, with validation checks in place.

The electronic records management system will then become the primary source for health records for the service.

7.2 Creation of Records

Wherever possible, within our services, patients will have a single, structured, multi-professional and agency record (SystmOne) which supports professional and integrated care.

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.

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

When creating a patient health record, it is important to check the Patient Master Index (PMI), which is part of the electronic system. This will determine whether the patient already has a case note number. The index should be searched properly, using as many different search criteria as possible. Once a complete search has been carried out, a patient can be added to the system with all the current patient demographics and a new number may be allocated and immediately added to the Patient Master Index. (Thorough checking of the system will prevent duplication of records) The key identifier for all patients is their NHS number. This should be given on the referral letter but should still be checked via the Summary Care Registration system (SCR) A manual record folder may also need to be created and should carry the appropriate details, including NHS number and Year Label (affixed on the right hand side).

When creating the record, if you are aware that another patient exists with the same name or details, a 'Same Name' label should be attached to alert future users. It is good practice to update the PMI, using free text, with the alert that another patient has the same name.

7.3 Front Cover of Paper-based Clinical Records

When any clinical record is created the following must be included on the front cover;

- Full Name – the patients/clients name must be clearly identifiable
- Identification Number – registration of a created record is the act of giving the record a unique identifier upon creation and addition to a record keeping system. Preferably this should be the patients/clients NHS number.
- NHS number
- Organisations and Service Identity
- Volume details – including date each record was opened and closed
- Private & Confidential

A newly created record should also include a signature sheet and filing instructions regarding filing of documentation and the order of this. Exemption to this is if a central signature sheet and/or filing instructions are kept within the service, clearly visible to all staff. This is to be agreed by the Information Governance Team and be documented within the services Local Record Procedure.

The signature sheet must include the signature, name and designation of all staff making entries within the patients/clients record. This must be completed when the member of staff makes their first entry within the record and the signature sheet is to be reviewed annually for accuracy and completeness.

Each sheet within the patients/clients record must clearly identify their name and unique identifier, preferably NHS number, where attainable.

7.4 NHS Numbers

As of September 2009 it was mandated that NHS numbers must be recorded on all active patient records and for all communication in relation to patient care. The NHS number will be used as the National patient identifier and will replace local identifiers, though it can be used in conjunction with local identifiers.

Patient safety is the key driver for this initiative. Correct and consistent usage of the NHS number eliminates duplicate records in clinical and patient administration systems. Service managers should ensure that appropriate staff receive training in order to be able to trace and verify NHS numbers for all patients.

All services should ensure that the NHS Number is stated on all clinical correspondence and verified when correspondence is received.

DSCN 31/2008 and DSCN 32/2008 state that no systems can be procured which does not enable the capture and validation of NHS numbers.

7.5 Completeness of Clinical Records

Part of the multi-disciplinary care process should be to audit the quality of clinical information on which decisions about the care of the patient are made. This should include a review of the completeness of information recorded, e.g. to ensure the inclusion of any information transferred in from other organisations or locations.

Records are written to assist/inform the decision making and problem solving process and should include;

7.5.1 **Care Plan**
A full account of the patients/clients assessment and the care that has been planned and provided must be documented within the record. Demonstrate that their care follows evidence-based guidance or supporting documents describing best practice, or that there is an explanation of any variance.

7.5.2 **Decisions Made**
Records must include the recording decisions, why they were taken, even if it is a 'wait and see' approach. Any advice sought from colleagues should also be recorded.

7.5.3 **Care Delivery**
Records must include the measures taken by the clinician to respond to patient's health needs.

7.5.4 **Information Shared**
Open and honest with the patient regarding entries, as far as practically possible, to ensure that all opportunities for health promotion are transferred to the patient

Written as much as possible in terms the patient/user can easily understand.

Records should include discussions with patients, e.g. prognosis or 'do not resuscitate' decisions.

7.6 Logging Queries
Patient: If a patient is unhappy with the decision for any reason, record this and the action taken to resolve the issue.

Internal Sources: Processes should be identified within the services for any queries from internal sources about entries in the health records and how these are to be logged

7.7 Quality of Clinical Records
Records must be;

7.7.1 **Indelible (Black Ink)**
Whether typed or handwritten this must be done in black ink.

It is recognised that some services may historically use differing ink colours e.g. Operation notes (red ink), Dental notes (Green ink), however approval should be gained from the Caldicott Guardian, via the Information Governance Team.

7.7.2 **Legible**
Clear and unambiguous
Not abbreviated due to potential ambiguity. Exceptions as per service areas approved List of Abbreviations (each service to hold).

7.7.3 **Factual**

Entries within records must be factual and personal views about the patient's behaviour or temperament should not be included unless these have a potential bearing on treatment.

7.7.4 **Dating and Timing**

In patient episodes must be dated and timed – (any omissions or later inclusions must be clearly dated and timed) N.B. this refers to date and time of entry to record Not date and time of any care or treatment which should be stipulated in the content of the reported entry should it be relevant to the report.

Contemporaneous (written within 24 hours or next working day).

Other services i.e. community can be identified from clinic attendance or diary entries for medication or care. Emergencies arising during a routine community attendance must be timed from onset.

Time should be recorded using 24hr clock. Where applicable both the time of patient interaction and the time of entry into record should be recorded

7.7.5 **Hypersensitivities and Alerts**

Hypersensitivities and other alerts are to be recorded in compliance with local policy documentation. This must be recorded in Red ink, signed and dated. This field must be completed, even if 'no known allergies or alerts' are stated.

7.7.6 **Signatures and Designations**

All entries must be signed. Signatures are to be supported by printed name and designation at least once on each page – unless a separate signature sheet exists containing this information.

7.7.7 **Unregistered / Non-Registered Staff**

All entries made by an unregistered member of staff.

Principles

1. Record keeping can be delegated to unregistered Health Care Professional so that they can document the care they provide.
2. Record keeping is an integral part of every intervention and the unregistered Health Care Professional should be assessed as competent in the complete provision of care, which includes record keeping. Until they are deemed wholly competent in both the activity and its documentation, countersigning as in principles four and five should be performed.
3. As with any delegated activity, the registered professional needs to ensure that it is in the patient's best interests for the activity and documentation to be delegated to the unregistered Health Care Professional.
4. Supervision and a countersignature are required until the unregistered Health Care Professional is deemed competent at the activity and keeping records.
5. Registered professionals should only countersign if they validate that the activity took place.

Countersigning: The key issues are:

- whether the Non-Registered Health Care Professional has been trained to appropriate standards and is competent to produce such records as part of the overall provision of care

- whether it is in the patient's best interests for recording of care (as well as care provision) to be delegated

If a registered professional is satisfied the above criteria are met, then delegation of the record keeping activity will be appropriate and there will be no requirement for the registered nurse to countersign the notes.

It is therefore a service decision to determine who is and is not competent to make record entries

7.7.8 **Loose Filing (Paper-based Records Only)**

All record documentation is to be bound and secured in a logical sequence within the record folder. There is to be no loose filing within clinical records.

No spaces to occur between entries. When starting a new page this should be referenced from previous one.

7.8 Verbal Communication

All verbal communication about patients care, treatment and support must be documented within the patient's record.

7.9 Patient Held Records

Patient held Records are defined as health records which are kept within the home of the patient or family

Patients should be advised that they should find an appropriate place in the home to store the record, where risk of damage is minimal (e.g. away from fire/flood)

If necessary, the patient should be given the option for the clinician to hold the record centrally, if for example, there is confidential information they do not wish others to view

When clinician's undertake their first consultation with the patient, they must discuss the confidentiality of the record. In order to do this, explain to the patient: why the record is being kept in the home, what storage conditions are suitable, what types of information will be recorded, who should have access to the record, when the record will be returned to the service and how this will happen.

Adult Patient Held Records: Once the care and treatment has been completed the Patient Held Record will be removed from the patient's home and follow the specific services arrangements in terms of storage, retention and disposal contained within the NHS medical Records Code of Practice.

Children Patient Held Records: Remain with parents, even after care has completed

7.10 Admissions process

An admission is where the health professional in charge of a patient's care admits the patient to a hospital bed for the purpose of treating or observing the patient's condition. This can be either as an elective planned or booked admission, or as an emergency.

The service/senior manager should ensure that the local inpatient procedures provide satisfactory documentation for the admission, treatment, transfer and discharge of the patient in line with national and local requirements.

On arrival, an admission form should be completed for inclusion within the patient medical record. This should include the following:

- Date of admission
- Place of admission
- Full name
- Date of birth
- Address (and post code)
- NHS Number
- Next of kin (and/or patient friend)
- Religion
- Ethnic group
- Registered GP
- Referring GP (source of referral)
- Source of admission
- Method of admission
- Brief description of reason for referral

The patient's ethnic group must be requested to inform the equality reporting of the NHS. The ethnic group must never be assumed and each patient should only be asked once during their admission.

Arrangements must be in place for receiving, recording and securely storing any patient property.

The patient must be informed that their information will be recorded and the ways in which it may be used and disclosed. The patient must be given the choice to restrict these uses or provide their consent. Specific consent must be sought for any uses which do not directly contribute to their healthcare. The patient should be made aware that they are permitted to have access to their own record and that their information will be protected.

7.11 Discharge Process

The Patient Administration System (PAS) Discharge Summary Form is used to inform the GP and patient of discharge details and procedures undertaken and gives a summary for inclusion in the patient medical record. This is also used for validation and clinical coding.

The ward must have appropriate procedures in place to ensure completion of the Discharge Summary Form (including filing and dispatch of copies), recording the return of patient property and issuing of a medical certificate (where appropriate).

The completed patient health record must then be returned to its correct home, either a local health records storage area or the central health records library as appropriate.

The health record should be tracked to its new location either by using the case note tracking functions on the Electronic system or by a manual tracer card.

Local procedures should be in place to ensure that, before returning the patient health record to its storage place, or it being passed on to a Medical Secretary, it is checked for completeness and order with appropriate labelling and sufficient blank stationery for the next appointment.

7.12 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.

7.13 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.

8 Clinical Records Management for Gender Reassignment Patients

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

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

2. 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.

3. The Human Rights Act also offers protection to individuals (whether or not that individual has obtained formal legal recognition in their acquired gender by being issued with a GRC).

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

5. 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.

6. 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.

7. 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.

8. 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).

9. 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.

Guidance for the handling of Transgender Patient's Medical Records

There are three categories of Transgender Patient Medical Records, all of which require different actions and communications with patients.

1. **Change of name (not by deed poll)**
   If a patient wishes to change the name they are known by e.g. from Jane Smith to John Smith, but **have not** done this by legal deed poll, they can have a "known by name" added to the medical records.

   The patient needs to be aware that their records will still identify them by their birth gender and their birth name will be on their record, but they can be referred to by their preferred name.

   No further action is required, with regards to the patients' medical records.

2. **Change of name (by deed poll)**
   If a patient wishes to change the name they are known by e.g. from Jane Smith to John Smith and **have** done this through a legal deed poll, they can apply for a new NHS Number.

   Once they have a new NHS Number the record will show their new name, but will still identify them by their birth gender.

   The Trust needs to recognise that the patient now has a new record. You can NOT merge the records automatically. The following things need to take place;

   - Provide the patient with a copy of their old medical records (Subject Access Request process should be followed)
   - The patient should meet with the HCP to discuss the content of their old medical record and what the HCP feels should be included in the new record. This should be agreed by the patient, if the patient does not agree, they need to be advised of the risks of this and a note recorded in the old record; the information can not be transferred into the new record.

- The HCP may want to consider writing a medical record summary to include in the new record. Again content agreed with the patient
- Copy the old record and redact information the patient does not wish to be shared (this could include the old NHS Number)
- The patient may be happy to merge the records with no redactions, but this is their choice

3. **Change of name and gender (following a gender recognition certificate)**
   If a patient has changed their name and gender, through a **gender recognition certificate**, they can apply for a new NHS Number.

   Once they have a new NHS Number the record will show their new name and new gender.

   The Trust needs to recognise that the patient now has a new record. You can NOT merge the records automatically. The following things need to take place;

   - Provide the patient with a copy of their old medical records (Subject Access Request process should be followed)
   - The patient should meet with the HCP to discuss the content of their old medical record and what the HCP feels should be included in the new record. This should be agreed by the patient, if the patient does not agree, they need to be advised of the risks of this and a note recorded in the old record; the information can not be transferred into the new record.
     - The HCP may want to consider writing a medical record summary to include in the new record. Again content agreed with the patient
     - Copy the old record and redact information the patient does not wish to be shared (this could include the old NHS Number and old gender, including anything that may identify their old gender)
     - The patient may be happy to merge the records with no redactions, but this is their choice

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

See Appendix D for Further Information

9 Clinical Records Management for Adopted Children

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 down and new record is opened.

10 Logically Deleted Process

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 can not merge the records nor copy over a complete set of the "logically deleted" record.

11 Effective Corporate Records Management

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.

11.1 Naming Folders, Files and Documents

Naming conventions are standard rules to be used for both naming documents and electronic folders and are designed to make it easier to find documents. Corporate standards must be followed in the naming of record files and folders. It is unacceptable for any documents to leave the organisation without having a logical filename or format for presentation that shows Solent NHS Trust as being the owner of the document. This corporate approach when applied to both paper and electronic files will ensure that current and future staff will be able to create, update and search for files efficiently.

File naming is critical with the move towards electronic document management (EDM). Files need to be named in a manner that is consistent and easily understood by all to avoid wasted time searching for documents in a large EDM or paper system.

11.2 Corporate Standards for Ownership of Documents

All records that are produced must adhere to the corporate standards for records and the following requirements should be applied:

1. The document must contain the Solent NHS Trust logo.
2. The document should specify

- author of the document
- the designation of the author e.g. *IG Lead.*
- The version number of the document
- The date the document was produced

11.3 The Key Five Naming Convention Principles

1. A date reference for when the file is saved to the system or updated, in the form of YYMMDD i.e. 190408 (this could also be YYYYMMDD 20190408), representing the 8th April 2019.

This order will mean that documents with the same titles but different dates will be shown in date order on electronic systems.

2. A file name description (normally the document title).Long words such as Management, organisation and department, should be shortened to Mgt, Org and Dept. The file name must represent the content of the document. The document status is appropriate if the document is in preparation e.g. labelled Draft.

3. A version number in the format e.g. V1.

4. DRAFT where applicable (version numbers must reflect the various stages of a draft record. If it is a draft of a new record the version number should be V0.1, V0.2, etc… If it is a draft of an existing record the version number should be V1.1, V1.2 or V2.1, V2.2, etc…)

5. The author of the document or their initials should also be included

6. The file extension (applicable to electronic records only)
This is normally allocated by the application i.e. doc or xls. In general, if you can see a file extension, there is no need to add one as it is assigned automatically by the application being used.

All electronic file names must exclude illegal characters. These include \/*?”’<>, Ideally

filenames should also replace a space with an underscore as this allows transfer to other computer systems keeping the file name intact. For example: 20190408_RecordsManagement&InformationLifecycle_Policy_Draft_V0.1_SB.doc

Alternatively spaces are acceptable where an email etc is being sent rather than a file being transferred.

11.4 Indexing Electronic Corporate Records

All Corporate Records must have a form of indexing, using the naming convention principles above and the File Pathway of the location of the record needs to be placed in the footer of the document. This will act as an identifier of where the record can be obtained. For example, R:\SolentNHSTrustInformationGovernance\Policies\20190804_RecordsManagementLifecycle_Policy_V4_SB.doc.

12 Security of Records

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

12.2 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.

12.3 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.

12.4 Access to storage facilities must be limited to designated staff

12.5 Records which have to 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.

12.6 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.

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.

13 Record Tracking Procedures

13.1 Clinical Policy

- All records movements will be tracked, either in paper format or electronically on the patient system (where this is used by the service).
- Individual departments/services will use an auditable tracking log to indicate the location of non electronic (e.g. paper records, x-rays) records if they are moved for any reason.
- Archiving and destruction of non-electronic/paper records will be tracked electronically.
- The NHS and/or hospital number will be used for tracking record movements.

13.2 Procedure for tracking other paper records

The tracking log may be manual.

Where electronic systems are not available tracking must be recorded using one of the following:

- Tracking Log
- Tracer card
- Diary
- Ledger

14 Data Quality

The Trust, service users and the public must have confidence in the quality of data used for the provision of patient care, information governance, management and planning, commissioning and accountability.

As Commissioners come to grips with an increasingly pressured funding regime, the organisations responsibility to report activity accurately and completely in a timely manner

has become central to its ability to receive funding for all the activity it performs. A significant amount of income is at risk if its data is not reliable and has poor data quality. In the context of the Care Quality Commission (CQC), this equates to lost income.

Initially there will be a particular focus on information from key information systems data, as there are real opportunities for increasing awareness of the importance of data quality and standardising data collection processes and procedures. This focus also falls in line with the national Information Quality Assurance Programme (IQAP) which currently primarily covers inpatient and outpatient data. The policy equally applies to all data held within the Trust.

The National Programme for IT demonstrates the importance the NHS itself places on data quality and as such is now incorporated into the Care Quality Commission Quality & Risk Profiles. This programme of work is well underway within the Trust and will facilitate the raising of data quality standards within the Organisation by providing, amongst other things, consistent and clear policies and procedures for staff to work to.

Poor quality data can create clinical risk, cause inconvenience to service users and staff, compromise effective decision making and impact on the Trust's ability to monitor standards of care and secure income for its services

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

15 Request for Records

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

16 Missing or Lost Records – Reporting an Incident

16.1 Definition

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, can not be located.

16.2 Procedure for Records that cannot be found – missing

The member of staff who identified the record as missing should report the missing record (this applies to records containing Personally Identifiable Data or Sensitive Data) to their supervisor/Line manager, work colleagues and Information Asset Custodian as soon as possible.

The supervisor/manager should ensure that a thorough search takes place. The place you would normally expect to find the record should be thoroughly searched, taking care to check either side above and below where it should normally be filed.

A colleague should also be asked to search separately in case it has been missed by you. Post the Number/Name (where no number) of the Missing record in a recognised but secure area, so that all relevant staff are aware of the incident.

Check recording systems (tracer cards/log books) and follow up.

If the record can not be located the event must be entered using the Electronic Incident reporting system, which will notify the Information Governance Team.

List the areas searched, and re-check a few days later as notes do sometimes re-appear.

If the record can still not be located a temporary record should be created both paper and electronically, clearly marked as a temporary record, populated with all relevant information available.

For clinical paper records temporary case notes should be set up and tracked on the electronic patient system (where applicable).

The person affected by the loss of the record should be informed. This should be documented in the new record and the Information Governance Team should be informed.

If original records are located the missing record log should be updated with details of where/how the original was located, and the two records should be merged both paper and electronically.

16.3 Unavailable clinical records

A record is regarded as unavailable if it is in use elsewhere and/or cannot be retrieved in time for an appointment or within 24 hours of admission.

The record is considered missing.

A temporary record should be created, as described in sections 16.2.

If an appointment or admission is deferred because the record is not available this should also be recorded on **the Incident Form**.

Reasons for records being unavailable may include:

- Record needed for another appointment/admission
- Record with Medical Secretary, Coding, Audit, Consultant, Information Team
- Record not tracked
- Misfiled
- Wrong record/volume/temp record(s) sent
- Patient has more than one hospital number
- Record lost in fire
- Patient unable to locate patient-held record
- Staff unable to retrieve records out-of-hours

If the record can still not be located it is consider lost and therefore an Incident Form/incident system must be completed

16.4 Records that do not arrive with a transferred patient

Where these records have not been traced or the record remains missing from the area which the patient has been transferred to for a period of longer than 24 hours. An Incident Form must be raised. Report any lost or missing records to the Information Governance Team.

Where a record has been subsequently traced refer to the missing record procedure in the first instance.

16.5 Breaches to Confidentiality

A record containing personally identifiable or sensitive data must be kept secure at all times and access restricted to appropriate and authorised personal. Any breaches or potential breaches of confidentiality must be reported using an **the online incident reporting system**.

16.6 Incident Reporting

When an Information Governance incident (or suspected incident) occurs staff should notify the Information Governance Team immediately.

The risk associated with Information Governance incidents will be measured using the Information Risk Incident Reporting System, which is part of the National Data Security & Protection Toolkit.

Specialist advice regarding information governance issues can be sought at InformationGovernanceTeam@solent.nhs.uk from the Information Governance Team or by contacting: 0300 123 3919.

The Information Governance Team has responsibility for:

- Reporting all IG incidents to the appropriate bodies including the Information Commissioner
- Reporting all IG Incidents to the appropriate responsible persons within Solent NHS Trust(i.e.) Accounting officer, Caldicott guardian & SIRO
- Investigating all IG SIRI's
- Collecting and investigating all forensic evidence
- Developing an action Plan
- play a key role in ensuring that as a provider organisation that we meet the performance requirements of the commissioning organisation
- produce SIRI reports showing trends
- discuss root causes and learning from these incidents at the Serious Incident Review Panel
- highlight any particular concerns / changes to practice, and the lessons learned, to Information Asset owners and Information Asset Custodians
- Re-training staff where an incident has occurred
- Privacy Impact Assessments are to be undertaken

Information Asset Owners have a responsibility to:

- investigate all reported SIRI's and inform the Risk Management Team of the outcome
- be aware of all SIRI's reported in their team/department
- raise any concerns regarding SIRI with the relevant Service Manager
- All suspected and actual Information Governance incidents must be reported within 24 hours to the Information Governance team (this can be done verbally)
- review the relevant risk assessments following a SIRI

17 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.

17.1 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.

17.2 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.

17.3 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.

17.4 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.

17.5 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.

17.6 All Staff

All staff under the Public Records Act, whether clinical or administrative, who create, receive and use records have records management responsibilities. In particular 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.

18 Failure to Comply with the Policy

If a service feels it can not comply with all or part of an IG policy/ procedure they have a duty to undertake a risk assessment (Appendix C) 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, (unless agreed exceptions have been approved) will result in disciplinary action, as stated within all staff contracts.

19 Training

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.

20 Equality & Diversity and Mental Capacity Act

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 E

21 Success Criteria/Monitoring the Effectiveness of the Policy:

The monitoring of this policy and its effectiveness and maintenance will be audited annually using the 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.

22 Review

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

23 Reference and Links to Other Documents

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

Policies:

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

Procedures:

- Registration Authority Procedure

Code of Practices:

- Destruction of Confidential Waste
- The Records Management Code of Practice for Health and Social Care 2016

Appendix A – Destroying or Retaining Records Outside of their Retention Period Form
Appendix B – Archiving Registration Form
Appendix C – Information Governance Risk Assessment

The above appendices can be located
http://intranet.solent.nhs.uk/TeamCentre/InformationGovernance/TeamDocument/Forms/Guidance%20%20leaflets.aspx

Appendix D – Gender Reassignment Patients

What the Laws says;

Equality Act 2010: The Equality Act protects people on the basis of gender reassignment from direct and indirect discrimination and harassment. This includes discrimination by association and discrimination against people perceived to have the *protected* characteristic of gender reassignment.

The Equality Act also places a proactive duty on public organisations to promote equality of opportunity, foster good relations and eliminate unlawful discrimination between people who have the protected characteristic of gender reassignment and people who do not.

The Equality Act 2010 states that - "A person has the *protected characteristic of gender reassignment* if the person is proposing to undergo, is undergoing or has undergone a process (or part of a process) for the purpose of reassigning the persons' sex by changing physiological or other attributes of sex."

The Government Equality Office guidance indicates – "The process of gender reassignment may involve different stages, from change of name, title and / or appearance through to surgical intervention. *However the Equality Act does not require a person to be under medical supervision to be "protected", so a woman who decides to live permanently as a man but who does not undergo any medical procedures will be protected.*

A wide range of people are included in the term "trans"; gender fluid, transgender, people who cross dress only on an occasional basis, and other people who may identify as neither men nor women, but somewhere in between. *Only persons who have obtained "protected characteristics of gender reassignment" are explicitly protected under the Equality Act 2010.*

Gender Recognition Act 2004: The Gender Recognition Act 2004 provides transsexual people with the opportunity to obtain legal recognition in their acquired gender by being issued with a Gender Recognition Certificate (GRC). Anyone with a GRC will be legally recognised for all purposes as their acquired gender. With someone who has a GRC, as you know, any disclosure of information without consent about that person's gender history may constitute an offence, unless by way of section 22 of this Act – (i) the disclosure is made to a health professional, (ii) it is made for medical purposes, and (iii) the person making the disclosure reasonably believes that the subject has given consent or cannot give consent. Further the exemption does not permit medical professionals passing on information freely about a "trans" individual's medical history.

Human Rights: Everyone has protected rights under the European Convention of Human rights (ECHR). Some of the articles which protect these rights have important relevance for transgender people.

Article 8 indicates that everyone has the right to respect for their private and family life. As such Article 8 will include gender identity within its scope. Article 8 can ensure that the personal and medical data of transgender people without GRC status is given the same respect and level of confidentiality.

Article 14 advocates non-discrimination on protected grounds such as sex, race, colour…gender, belief etc. It is therefore essential that Human Rights are taken into account when delivering services.

Guidance: It is important that transgender individuals do not experience discrimination in the clinical setting. Medical professionals should use names and titles that the individual concerned regards as

appropriate. If the situation is unclear, medical staff should discuss these issues with the individual privately.

Confidentiality is an especially sensitive issue for transgender individuals. Consequently it is the position adopted by the Department of Health and NHS generally that "no non-essential disclosure of an individual's transgender status or history should occur".

Whether there is a GRC or not, clinicians who need to pass on details to other medical staff should ask themselves –

- Is the information regarding the patient's present or past gender status or gender treatment relevant to the circumstances?

- What would be the purpose of passing on such information – is it medically relevant?

- Is there a way of providing information that is relevant without necessarily referring to the individual's transgender identity or history?

- Have names and pronouns been chosen so that the patient history around gender is not inadvertently exposed.

For example, it would be unacceptable if a clinician is referring a transgender woman to another medical professional for carpel tunnel syndrome to indicate in the referral letter that the patient used to be a man.

The question as to managing medical records more widely is a difficult one and can be a challenge for clinicians and medical staff. Names and titles on medical records may be changed at the point that an individual changes their gender role *permanently or sooner if this is requested, and there is some evidence of the intended permanency of the change*.

Whilst clinicians can change an individual's name on their electronic folder or paper file, individual notes contained within these may not be changed because this may put health at risk.

However, letters and envelopes should be addressed in accordance with that new identity (unless the individual specifically requests otherwise).

The above ties in which NHS Guidance which indicates that "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".

Further, a transgender individual can request that access to (electronic) sensitive information is blocked by the organisation which created the record so that access is limited to medical professionals only and receptionists / administrative staff for example will not be able to access the same level of information that a medical professional (i.e. doctor) could.

Although NHS guidance recognises that the practicality of a name change may lead to risks; there is not a great deal of clarity as to how those risks should be managed.

Appendix E – Equality Statement

Step 1 – Scoping; identify the policies aims	**Answer**
1. What are the main aims and objectives of the document?	To outline the process for creating, reviewing and records and Information management standards within Solent NHS Trust
2. Who will be affected by it?	All staff who are developing records
3. What are the existing performance indicators/measures for this? What are the outcomes you want to achieve?	N/A
4. What information do you already have on the equality impact of this document?	None
5. Are there demographic changes or trends locally to be considered?	N/A
6. What other information do you need?	N/A

Step 2 - Assessing the Impact; consider the data and research	**Yes**	**No**	**Answer** (Evidence)
1. Could the document unlawfully against any group?		x	
2. Can any group benefit or be excluded?		x	Applies to all staff groups
3. Can any group be denied fair & equal access to or treatment as a result of this document?		X	N/A
4. Can this actively promote good relations with and between different groups?		X	N/A
5. Have you carried out any consultation internally/externally with relevant individual groups?	X		Current Policy Steering Group members consulted
6. Have you used a variety of different methods of consultation/involvement	X		Via email and face to face
Mental Capacity Act implications			
7. Will this document require a decision to be made by or about a service user? (Refer to the Mental Capacity Act document for further information)	X		Does not apply to patients
External considerations			
8. What external factors have been considered in the development of this policy?	X		Legislation
9. Are there any external implications in relation to this policy?	X		Legislation
10. Which external groups may be affected positively or adversely as a consequence of this policy being implemented?			All positively, open access to information, within legal perimeters