Somerset Partnership NHS
NHS Foundation Trust

RECORD KEEPING AND RECORDS MANAGEMENT POLICY

(Clinical and Corporate Records)

Version:	5
Ratified by:	Senior Managers Operational Group
Date ratified:	August 2015
Title of originator/author:	Information Governance Manager
Title of responsible committee/group:	Caldicott & Information Governance Group
Date issued:	**August 2015**
Review date:	**July 2018**
Relevant Staff Groups:	All Trust Staff working with any form of record, Trust agents and contractors also working with Trust records

This document is available in other formats, including easy read summary versions and other languages upon request. Should you require this please contact the Equality and Diversity Lead on 01278 432000

DOCUMENT CONTROL

Reference	**Version**	**Status**	**Author**
PA/Aug15/RKRM	5	Final	Information Governance Manager
Amendments	Amendments incorporated from Head of Corporate Governance		
Document objectives: To form an over-arching and robust single Record Management policy that is compliant Trust-wide for all Trust record activity.			
Intended recipients: Senior and Team Managers specifically; all Trust staff and temporary staff bank or agency staff, locums, students or volunteers) working with any Trust record either clinically, corporately or generally.			
Committee/Group Consulted: Caldicott and Information Governance Group.			
Monitoring arrangements and indicators: Information Governance Toolkit requirements monitored through the Caldicott and Information Governance Group.			
Training/resource implications: General awareness for all Partnership Foundation Trust staff. Specific training from the Information Governance Team accessed through Senior Manager(s).			
Approving body and date	Caldicott & Information Governance Group	Date: August 2015	
Formal Impact Assessment	Impact Part 1	Date: August 2015	
Clinical Audit Standards	YES	Date: TBA	
Ratification Body and date	Senior Managers' Operational Group	Date: August 20115	
Date of issue	**August 2015**		
Review date	**July 2018**		
Contact for review	Information Governance Manager		
Lead Director	Director of Governance and Corporate Development		

CONTRIBUTION LIST Key individuals involved in developing the document

Name	**Designation or Group**
Phil Brice	Director of Governance and Corporate Development
Tricia Oliver	Information Governance Officer
Andrew Sinclair	Equality and Diversity Lead (for Policy documents)
Sue Balcombe	Caldicott Guardian
C&IGG	Caldicott & Information Governance Group
Liz Berry	Senior Nurse Clinical Practice
All Members	Clinical Policy Review Group

CONTENTS

1 Introduction

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

The Trust's records are its corporate memory, providing evidence of actions and decisions and representing a vital information 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.

Clinical record keeping is an integral part of clinical care. It is a significant tool of professional practice and is essential for the delivery of safe patient care. It is not an optional extra to be fitted in if circumstances allow (NMC 2009). The quality of record keeping is a reflection of the standard of professional practice, whether the records are paper or electronic. A good standard of record keeping is the mark of skilled and safe practitioners.

This document sets out a framework within which the staff responsible for managing the Trust'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.

The policy also identifies the standards expected for clinical record keeping. It sets a minimum standard, which will be applicable to all patient settings, and also occasions when staff are required to write in the records of other providers of care. These guidelines do not replace the standards set by professional organisations but are complementary to them.

This policy document should be read in conjunction with the Trust's Records Management Strategy which sets out how the policy requirements will be delivered.

The Trust Board has adopted this record keeping and 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:

- The provision of safe and effective patient care
- better use of physical and server space;
- better use of staff time;
- improved control of valuable information resources;
- compliance with legislation and standards; and

- reduced costs.

2 PURPOSE AND SCOPE

The purpose of this policy is to provide guidance on the procedures and standards required to ensure that records are managed and controlled effectively, commensurate with legal, operational and information needs, and to enable safe and effective patient care.
This policy relates to all clinical and non-clinical (Corporate Records) operational records held in any format by the Trust. These include:

- all administrative records (e.g. personnel, estates, financial and accounting records, notes associated with complaints); and
- all patient health records (for all specialties and including private patients, including x-ray and imaging reports, registers, etc.)

This policy applies to all staff employed by Somerset Partnership NHS Foundation Trust as well as other health and social care staff such as temporary staff, students, locums and volunteers who document in clinical, and/or non-clinical operational records.

3 EXPLANATIONS OF TERMS USED

Records Management is a discipline which utilises an administrative system to direct and control the creation, version control, distribution, filing, retention, storage and disposal of records, in a way that is administratively and legally sound, whilst at the same time serving the operational needs of the Trust and preserving an appropriate historical record. The key components of records management are:

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

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

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

Information is a corporate asset. The Trust's records are important sources of administrative, evidential and historical information. They are vital to the Trust to support its current and future operations (including meeting the requirements of Freedom of Information legislation), for the purpose of accountability, and for an awareness and understanding of its history and procedures.

4 AIMS OF OUR RECORDS MANAGEMENT SYSTEM

The aims of our Records Management System are to ensure that:

- **records are available when needed** - from which the Trust 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** - using consistent and documented retention and disposal procedures, which include provision for appraisal and the permanent preservation of records with archival value; and

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

5 DUTIES & RESPONSIBILITIES

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 Department of Health: Records Management NHS Code of Practice. This will couple with:

- The Public Records Act 1958;
- The Data Protection Act 1998;
- The Freedom of Information Act 2000;
- The Common Law Duty of Confidentiality;
- Access to Health Records Act 1990
- Regulation of Investigatory Powers Act 2000

- The NHS Confidentiality Code of Practice.
- NHS Information Governance: Guidance on Legal and Professional Obligations
- Code of Practice 'BIP 0008-1:2008: Evidential weight and legal admissibility of information stored electronically
- Any new legislation affecting records management as it arises from either the Lord Chancellor, the Information Commissioner or a Secretary of State.

5.2 The **Chief Executive** has overall responsibility for records management in the Trust including clinical records. As Accountable Officer he/she 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 is personally accountable for the quality of records management under the terms of the Public Records Act (1958 S.3).

5.3 The **Trust Directors** have a particular responsibility for ensuring that the Trust corporately meets its legal responsibilities, and for the adoption of internal and external governance requirements. Relevant Directors of the Trust are personally accountable for the quality of records management under the terms of the Public Records Act (1958 S.3).

5.4 **Directors and Heads of Service,** as senior information asset owners, are personally accountable for the quality of records management within the Trust, and all line managers must ensure that their staff whether administrative or clinical are adequately trained and apply the appropriate guidelines. Staff must have an up-to-date knowledge of the laws and guidelines concerning confidentiality, data protection and access to health records. Responsibility for records management matters will be co-ordinated and delegated through directors, Heads of service and service leads. Each Director and manager will be responsible for implementing local records management procedures, in accordance with this Record Keeping and Records Management Policy.

5.4 The **Director of Governance and Corporate Development** is the Executive Lead for this policy and will ensure policy development and review takes place at least every three years, or sooner in line with local and national guidance. Ensuring that the Records Keeping and Records Management Policy and Strategy are implemented and that the records management system and processes are developed, coordinated and monitored.

5.5 The Trust's **Caldicott Guardian** is the Director of Nursing and Patient Safety, and has a particular responsibility for reflecting patients' interests regarding the use of personal confidential data. They are responsible for ensuring personal confidential data is shared in an appropriate and secure manner.

5.6 The **Senior Information Risk Owner** (SIRO) is the Director of Finance and Business Development; the designated Executive Director with responsibility

for coordinating the development and maintenance of information risk management policies, procedures and standards for the Trust. The SIRO is responsible for the on-going development and day-to-day management of the Trust's Risk Management Programme for information privacy and security.

5.7 The **Data Protection Officer** is the Director of Governance and Corporate Development; the designated Executive Director with responsibility for overseeing compliance with the Data Protection Act 1998 and co-ordinating responses to requests for disclosure of personal data under the provisions of the Act.

5.9 The **Information Governance and Records Manager** is accountable to the Director of Governance and Corporate Development and the Caldicott Guardian for overseeing the Trust's compliance with the Freedom of Information Act 2000 including the dissemination of information and section 46 of the Public Records Act ;co-ordinating responses to requests for disclosure of information requested under the provision of the Act; and overseeing the Trust's compliance with the Data Protection Act 1998 and for co-ordinating responses to requests for disclosure of personal data under the provisions of the Act.

5.10 **Information Asset Owners** (IAO) are designated senior managers, who are responsible for ensuring that information risk assessments are performed at least once each quarter on all information assets where they have been assigned 'ownership', following guidance from the SIRO on assessment method, format, content, and frequency. IAOs must submit the risk assessment results and associated mitigation plans to the SIRO for review, along with details of any assumptions or external dependencies. Mitigation plans must include specific actions with expected completion dates, as well as an account of residual risks.

5.11 **Heads of Divisions/Service/Team/Ward Managers and Matrons** have responsibility for ensuring the quality of clinical records generated by their staff, and monitoring compliance with this policy through the supervision process.

5.12 All staff who work for or individuals working on behalf of the Trust are responsible for any records which they create or use in the performance of their duties. Any record that an individual creates is a public record and will be subject to both legal and professional obligations. This responsibility is established and defined by the Public Records Act 1958. Everyone who records, handles, stores, or otherwise comes across information has a personal common law duty of confidence to patients and to his or her employer. The duty of confidence continues even after the death of the patient or after an employee or contractor has left the NHS.
Temporary staff such as bank or agency staff, locums, students or volunteers must be advised about the Trust's requirements for record keeping as part of their induction on arrival. It is the duty of the permanent staff handing care of patients to temporary staff to ensure that they are made aware of their responsibilities for record keeping.

5.13 The **Trust Best Practice Groups** are responsible for monitoring the results of record keeping related compliance audits and agreeing and implementing actions plans where appropriate.

5.14 The **Caldicott and Information Governance Group** is responsible for monitoring overall compliance with this policy. Any changes to this policy will be approved by this Group; the policy will be reviewed every three years or sooner if national or local guidance requires.

5.15 The **Clinical Governance Group** is responsible for the monitoring of compliance with the clinical records element of this policy, where records are held in paper or electronic form.

6 RECORDS MANAGEMENT INFORMATION LIFECYCLE FRAMEWORK

The following sections detail the lifecycle of a record, within a paper or electronic information systems. The **record** lifecycle defines five distinct phases:

1. Creation;
2. Retention;
3. Maintenance;
4. Use; and
5. Disposal

This policy covers the details for each of these phases and the Trust's employees' obligations under this policy. This policy covers the obligations of all staff employed by the Trust, all organisations contracted to the Trust and any organisation, or third party, which share Person Confidential Data (PCD) within the Trust.

To assist staff in adhering to this policy Appendix A has links to procedures, protocol for each stage of the record lifecycle (sections 6.1–6.5) You are expected to follow the requirements of these procedures and protocols. If this is not practical, you are expected to contact the Information Governance Team to seek advice before taking alternative action.

6.1 Record creation and the registration of records collection.

The Trust has established and maintains mechanisms through which departments and other units **must** register the records they are maintaining. This is contained in an Information Asset Register (IAR). This Information Asset Register will facilitate:

- the classification of records into series
- the recording of the responsibility of individuals creating records
- The Information Asset Register must be review annually by all department(s) IAOs.
- Employees should consider the following when creating information:
- what they are recording and how it should be recorded;

- why they are recording it;
- how to validate information (with the staff, patient or carers or against other records) to ensure they are recording the correct data;
- how to identify and correct errors and how to report errors if they find them;

6.1.1 Record creation tracking mechanisms must be put in place

Staff should understand what the records are used for and therefore why timeliness, accuracy and completeness of recording is so important; and
- how to update information and how to add in information from other sources
- tracking & retrieval system

When records are retrieved or removed for any reason from the file storage system, their removal and subsequent return should be recorded using a robust tracking system. As a minimum it should include:

- The unique identifier (NHS Number in the case of clinical records)
- A description of the item
- The name of the individual requesting and the reason for the request
- The person or department to whom it is being sent
- The date of transfer
- The date of return
- The signature and printed name of the person returning the file

In order to provide an effective retrieval service, it is essential that the movement of all patient records are recorded either on an electronic system; on a suitable database for manual tracking systems.

Electronic tracking of records through current systems and through off-site storage should be used to record and monitor movement of records, where staff have access to it.

Link to procedures for Record Creation

6.2 Record Retention

It is a fundamental requirement that the organisation's records are retained for a minimum period of time for legal, operational, research and safety reasons. The length of time for retaining records will depend on the type of record and its importance to the organisation's business functions.
Keeping unnecessary records wastes staff time, uses up valuable space and incurs unnecessary costs. It also imposes a risk liability when it comes to servicing requests for information made under the Data Protection Act 1998 (DPA) and/or the Freedom of Information Act 2000. Moreover, compliance

with these acts means that, for example, personal data must not be kept longer than is necessary for the purposes for which it was collected. Records should only be destroyed as per Somerset Partnership NHS Foundation Trust policy. It can be a personal criminal offence to destroy requested information under either the Data Protection Act (Section 61) or the Freedom of Information Act (Section 77). Therefore, Somerset Partnership NHS Foundation Trust needs to be able to demonstrate clearly that records destruction has taken place in accordance with proper retention procedures. The Code of Practice on Records Management, issued under Section 46 of the Freedom of Information Act 2000, requires that records disposal 'is undertaken in accordance with clearly established policies that have been formally adopted'. The Records Retention Schedule is a key component of Somerset Partnership NHS Foundation Trusts information compliance and allows it to standardise its approach to retention and disposal.

6.2.1 Records involved in Investigations, Litigation and Legal Holds

A Legal hold, also known as a litigation hold, document hold, hold order or preservation order is an instruction directing employees to preserve (and refrain from destroying or modifying) certain records and information (both paper and electronic) that may be relevant to the subject matter of a pending or anticipated lawsuit or investigation. Organisations have a duty to preserve relevant information when a lawsuit or investigation is reasonably anticipated. Staff must immediately notify the Information Governance & Records Manager and the Claims and Litigation Manager if they have been notified of a Litigation or Investigation or have reasonable foresight of a future Litigation or Investigation as this could result in records being held beyond their identified retention period.

Link to Records Retention Procedures

6.3 RECORD MAINTENANCE

All information needs to be maintainable through time. The qualities of availability, accessibility, interpretation and trustworthiness must be maintained for as long as the information is needed, perhaps permanently, despite changes in format. The use of standardised filenames and version control methods should be applied consistently throughout the life of the information.

6.3.1 Tandem electronic and paper records

For the avoidance of doubt no new *paper* patient clinical health record can be created **where a full electronic record exists**. The exceptions to this are clinical work that falls outside of the main electronic system and there is a requirement to record that information either to protect the patient or ensuring clinical care has taken place; such as charts or clinical entries where the main system does not allow for input of that information or, as 'Working Notes'.

- Where there is a requirement for a paper health record as no electronic system is available that meets the Trust's needs, then the following

apply:Paper health records must be formatted in the Trust approved manner/format

- For records less than six sections this can be a single record but six sections or over requires formal partitions and a contents/index at the front of the document e.g. demographics/historical information/clinical or other risks/running record/x-rays/reports/correspondence etc.
- The record must be in logical order
- There must be a unique reference number which, where a joint PAS system is in place must also link directly to that PAS number

The Trust operates a range of Electronic Patient Record systems across a broad range of services. All electronic systems have been developed in accordance with contractual arrangements and each record system is compliant with the NHS Record Management: Code of Practice and the NHS Information Governance Toolkit requirements (as applicable). Therefore, the creation of a blank record set (within each system) follows a consistent format, in line with contractual specification. A record is created within the system once clinical activity is initiated.

Electronic health records are held on Trust servers or approved external servers and not held on stand-alone devices and do not need tracking mechanisms. Tracing records is provided within the clinical system as required using search facilities but not via generic internet search engines.

Paper health records must have track and trace facilities as they may be transferred to other clinicians or placed into storage (archiving) and a system is required to be able to find the record(s) when required. This includes:

- Ensuring a log of those records is held locally or accessible for the local team if a central electronic system is used – see 5.12 and 5.13

Where track and trace cards are used these must have sufficient information in order to be able to clearly identify the health record and where it has been transferred to and who is responsible for that record when received (normally the clinician who requested the record)

For Patient Administration Systems (PAS) these will, wherever possible, be amalgamated into a combined patient record and integrated PAS record system (such as RiO). Stand-alone PAS systems such as Cerner will continue to operate unless the clinical work can be better met within the (RiO) electronic health record system.

6.3.2 Retrieving records – both clinical and non-clinical

Retrieving a record can be either:

- For immediate work, e.g. to update a record during an episode of care
- Finding an active file for clinical purposes
- To find archived information

6.3.3 Requesting archived records (retrieval)

Community and Mental Health Directorate records will be requested through the Information Governance Team or through the Record (Bank) staff at the main paper health record store on the Wellsprings site.

6.3.4 Storage of Records

All manual and electronic records in the organisation must be appropriately stored and retained in accordance with recommended retention periods.

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

Records must always be kept securely with appropriate security measures in place to prevent loss, unauthorised access and modification, but a balance needs to be achieved between security and accessibility. Storage accommodation for current records should be clean and tidy, and it should prevent damage to the records.

Equipment used for active records should provide storage which is safe from unauthorised access and which meets fire regulations, but which allows maximum accessibility to the information commensurate with its frequency of use. The following factors must be taken into account:

- compliance with health and safety regulations
- degree of security required
- users' needs
- type of records to be stored
- size and quantity of record
- usage and frequency of retrievals
- ergonomics, space, efficiency and price

6.3.5 Scanned Records

When paper records are scanned in order to be stored electronically it is important that there are processes in place to check the quality and accuracy of the scanning process and the quality and integrity of the final scanned record. Appropriate backup systems must be in place for any systems that include scanned records. Original records should not be disposed of until the quality of the scan has been checked

Link to Scanning Documents

6.3.6 Records in Patient/Service User's Homes

In some circumstances records may be stored at the patient/service user's home, e.g. district nursing care plans. They must be returned to the base when no longer in use. Stored records should be made safe whenever they are left unattended. Ideally they should be protected by additional security

such as being locked up and keys made available to authorised staff only. However, confidentiality of records left in the patient/service user's home is the responsibility of the patient/service user and they must be informed of this.

Link to Record Maintenance Procedures

6.4 Record Use

All information must be used consistently, only for the intentions for which it was intended and never for individual employee's personal gain or purpose. If in doubt employees should seek guidance from the Information Governance Team.

Patients have the right the right under the Data Protection Act to ask for a copy of the information that we hold about them. This is known as a Subject Access Request. Please follow the procedures in appendix A.

6.4.1 Filing

Each area where notes are stored should have clear filing guidance. All documentation should be stored in the appropriate filing systems when not in use. Filing documentation is the responsibility of the individual who last made an entry in the record or by their relevant and trained administrative staff.

Complaints or litigation papers should always be filed separately from clinical records

File copies of letters do not have to be signed.

6.4.2 Confidentiality and Security of Information

Unauthorised disclosure or misuse of information contained in records constitutes a serious breach of conduct that may lead to disciplinary action, and is also a criminal offence under Section 55 of the Data Protection Act 1998. Staff must guard against breaches of confidentiality by protecting information from improper disclosure and use at all times.

The Data Protection Act 1998, Professional Codes of Conduct, Human Rights Act 1998, administrative law and common law duty of confidentiality all place responsibility on everyone to maintain confidentiality of personal information. ('Confidentiality: NHS Code of Practice' provides further guidance and applies to all NHS employees URL Link))

Basic principles that should be adhered to are as follows:

- Records should never be left in a position where unauthorised persons can obtain access to them (including computer screens left on but unattended)
- Only staff who are authorised to access patient/service users records as part of their duties in or associated to the provision of care and treatment, or in carrying out audit and governance duties, are permitted to do so.

- The content of records should not be communicated with persons not authorised to receive them. They may be discussed on a need to know basis only to provide care and treatment to the patient/service user.
- Correspondence between the organisation and staff/patient/service users about staff/patient/service users should be clearly marked 'Confidential' to ensure confidentiality.

6.4.3 Information Sharing

National policy developments, highlights the need for health and social care to work together to provide seamless services to patients wherever the need arises. This has important implications for sharing information between health and social care. This was confirmed within the Health & Social Care Act 2012 and the Caldicott 2 Review (To Share or Not to Share).

As an NHS organisation, we increasingly need to seek assurances that our social care partners apply the equivalent information security standards to their own information assets and vice versa. Where cross-boundary NHS information sharing arrangements are required, the implementation of relevant and consistent standards for information security management provides the basis that underpins trust and confidence in these partnership arrangements.

Person confidential data will be shared in line with legislation, national guidance and documented information sharing agreements which have been agreed through the Trust's Information Governance processes.

6.4.4 Transporting Records

The mechanism for transferring information from one organisation to another should also be tailored to the sensitivity of the material contained within the records and the media on which they are held.

Health records or other confidential information for transportation between Trust sites/departments or to other health organisations within the Local Health Community and social care, must be enclosed in sealed bags /envelopes/designated secure boxes and labelled appropriately i.e. confidential, and sending location included in order to aid return. For specific situations of extreme sensitivity e.g. child protection, a further statement should be added stating 'to be opened by addressee only'.

Records must be carried between sites/departments by authorised staff only. Authorised staff may include:

- Appropriate member of staff
- Internal transport systems
- Authorised courier service
- Off-site records storage supplier
- Special Delivery by Royal Mail

Where external courier services are used to transfer staff/patient/service user records between health organisations, a formal contract needs to be put in

place including ensuring that the documents are transported in sealed envelopes. The contract should include confidentiality issues. A schedule of documents should be presented to the courier for signature which should be cross-checked by the organisation receiving the records.

Employees must not send health records by first class mail. Appendix A sets out a process to assist in making decisions about the appropriate transport mechanism and media.

Records should not be left unattended in transit at any time. When carried in a car they must be locked in the boot.

Only in exceptional circumstances may records be taken home by a member of staff to work on. Where this is necessary, a risk assessment should be undertaken and arrangements put in place to ensure that they are kept secure.

Evidence of this risk assessment should be held locally by the service, with authorisation from the lead for the service. Staff who do take records home will be responsible for the security and confidentiality of the records (See Appendix A Guidance for Staff carrying records off site).

Transporting records from Trust premises requires vigilance and the principles of confidentiality must be maintained.

Records selected for archival preservation and no longer in regular use by Somerset Partnership NHS Foundation Trust should be transferred to an archival institution, for example a 'Place of Deposit'. This must be approved by The National Archives and have adequate storage and public access facilities.

Following implementation of the Constitutional Reform and Governance Act 2010, in particular Part 6: Public Records and Freedom of Information, non-active records are required to be transferred no later than 20 years from the creation date of the record, as required by the Public Records Act 1958.

The Information Governance Manager Records Manager will identify Somerset Partnership NHS Foundation Trust "Place of Deposit" and assist in the transfer of those records identified.

6.4.5. Record Closure

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

The storage of closed or non-current records awaiting disposal should follow accepted standards relating to environment, security and physical organisation of files.

Link to Record Use Procedures

6.5 Record Disposal

It is particularly important under freedom of information legislation that the disposal of records, which is defined as the point in their lifecycle when they are either transferred to an archive or destroyed, is undertaken in accordance with clearly established policies which have been formally adopted by the Trust and which are enforced by properly trained and authorised staff.

- disposed of appropriately – using consistent and documented retention and disposal procedures, which include provision for appraisal and the permanent preservation of information with archival value.
- information lifecycle management is the responsibility of all staff and therefore managers are responsible for ensuring weeding exercises to review information held within departments are undertaken on a regular basis.
- destroyed appropriately – records can contain sensitive or confidential information. It is therefore vital that confidentiality is safeguarded at every stage and that the method used to destroy records is fully effective and secures their complete illegibility and inability to be reconstructed. Any records that have been identified for destruction must be destroyed as soon as possible after they are eligible.

Link to Record Disposal Procedures

Failure to comply with the statements in paragraph 6.1 – 6.5 could result in reputational damage to Somerset Partnership NHS Foundation Trust and carries financial penalties of up to £500,000 imposed by the Information Commissioner. This policy applies to all employees and must be strictly observed. Failure to do so could result in disciplinary action.

7 CLINICAL RECORD KEEPING

Good clinical record keeping is an integral part of professional practice and is essential to the provision of safe and effective care. As well as individual Professional Codes of Practice there are also national standards and regulations that must be met to ensure good clinical record keeping practice. These include:

Care Quality Commission: Essential standards for safety and quality. Outcome 21 details requirements for Record Keeping.

NHS Litigation Authority – Risk Management Standards: These are designed to address organisational, clinical, and non-clinical, health and safety risks.

Information Governance Toolkit: Information Governance covers the way organisations ‘process’ or handles information and includes both corporate and clinical information. The Information Governance Toolkit draws together the legal rules and central guidance and presents them in one place as a set of information governance requirements.

7.1 Record Keeping Functions

Good record keeping has many important functions. These include:

- Helping to improve accountability
- Showing how decisions related to patient care were made
- Supporting the delivery of services
- Supporting effective clinical judgements and decisions
- Supporting patient care and communications
- Supporting the involvement of the patient in their own health care
- Making continuity of care easier
- Providing documentary evidence of services delivered
- Promoting better communication and sharing of information between members of the multi-professional healthcare team
- Helping to identify risks, and enabling early detection of complications
- Supporting clinical audit, research, allocation of resources and performance planning
- Helping to address complaints or legal processes

7.1.1 Types of Clinical Records

The principles of good record keeping apply to all types of records, regardless of how they are held. These include:

- Handwritten clinical notes
- Electronic health records (including scanned records)
- Emails
- Letters to and from health professionals
- Laboratory reports
- X-rays
- Printouts from monitoring equipment
- Incident reports and statements
- Photographs
- Audio Visual media e.g. audio and video tapes, digital recordings, CDs and DVDs
- Tape-recordings of telephone conversations
- Text messages

7.2 Record Keeping Standards

Staff must keep clear, accurate and legible records, reporting the relevant clinical findings, the decisions made, the information given to patients, and any drugs prescribed or other investigation or treatment.

Clinical records must provide a safe and effective means of communication between appropriate members of the health care team - including the patient themselves. It is important that all records are able to be identified and traced in order to provide prompt access to them when required.

Clinical records must:

- Be written clearly, legibly and in such a manner that they cannot be erased.
- Be accurately dated, timed and signed, The signatory's designation / role must also be recorded
- Be recorded as soon as possible after an event has occurred, providing current information on the care and condition of the patient. This should be within 24hours, if not, the reasons for the delay must also be recorded. An entry should never be made in advance (unless it is a plan).
- Be complete, consistent, accurate and consecutive
- Be factual and not include unnecessary abbreviations, jargon, meaningless phrases or irrelevant speculation. If abbreviations are used, they must be written in full the first time used e.g. Care Quality Commission (CQC) or from an approved abbreviation list. This approved abbreviation list must be held in any patient record they are used in. 'Left' and 'Right' should always be written in full
- Only state relevant and useful information
- Identify any risks or problems that have arisen and the action taken to rectify them
- Be written, wherever possible, with the involvement of the patient, carer or parent
- Be held securely and confidentially
- Be used for the purpose for which it was obtained and only shared appropriately and lawfully
- Be readable when photocopied or scanned
- Be bound and stored so that loss of documents is minimised

In addition, erasers and liquid paper must not be used to cancel errors on paper records. A single line must be used to cross out and cancel mistakes or errors and this must be signed and dated by the person who has made the amendment. The original entry must remain legible,

Clinical records <u>must not</u>:

- Include any coded expressions of sarcasm or humorous abbreviations to describe the patient / client
- Be kept for longer than is necessary

7.2.1 Students

All entries made by student nurses and student Allied Health Professionals must be checked for accuracy and appropriateness, and countersigned by an appropriate professional

7.3 Clinical records must include:

- Registration / referral details of the patient. Information recorded must include: first name, last name, date of birth, NHS Number, address including post code, contact telephone number, gender, ethnicity, GP

details and next of kin details. This information must be checked regularly to ensure it is up to date and accurate
- Medical observations: examinations, assessments, tests, diagnoses, prescriptions, other treatments.
- Other relevant information / forms / assessments such as Assessment of Capacity (Mental Capacity Act), Lasting Power of Attorney, Advanced Directives or Statements
- Evidence of the care planned, risks assessed, the decisions made, the care delivered and the information shared
- Evidence of actions agreed with the patient, including consent to treatment and / or consent to share information
- Relevant disclosures by the patient – pertinent to understanding the cause or affecting the care / treatment of the illness
- Details of facts and information given to the patient
- Correspondence to and from the patient and / or other parties
- Discharge / Transfer of Care documentation

It is important that all aspects of the record must be identifiable to the particular patient so every page must contain, at least, the following patient details:

- First Name,
- Last Name,
- NHS Number and,
- Date of Birth.

8 CORPORATE RECORDS REQUIREMENTS

Corporate electronic records including Human Resources, Finances, Facilities, Corporate Management (including Risk systems) must all be fit for purpose and comply with national requirements that govern the area of activity in question. All electronic records that could be used in Court, or be required for any other legal activity or as evidence of compliance to a standard must comply with the Information governance Toolkit requirements of admissible evidence. This includes (but is not limited to):

- Staff training records.
- Staff records (general).
- Incident reports.
- Litigation or advice from Trust solicitors.
- Building and environmental records.
- Finance records.
- Audit reports.

8.1.1 Requesting archived corporate records (retrieval)

Corporate records should be requested through nominated leads for the directorate in question, e.g. HR, Finance or Facilities. These leads will advise if direct requests for information can be made through the Information Governance & Records Manager.

Link to procedures for Corporate Record Creation

9 INCIDENTS AND LOST RECORDS

Any incident or near miss relating to a breach in the security regarding use, storage, transportation or handling of records must be reported using the organisation's Incident recording via DATIX accessible to all staff on the Trust Intranet.

A serious breach of security e.g. major theft or fire must be managed in accordance with the same Policy in relation to it being a Serious Incident Requiring Investigation (SIRI).

The organisation's Information Governance Manager must be informed immediately of any loss or misplacement of any document that is used to record service user information, including diaries, or organisational business. When all efforts to locate the record have been exhausted, an incident form must be completed giving clear details of all actions including:

- when and where the record was last seen, with date known
- if stolen, from where and Police Incident Number
- actions taken to locate file

It is the responsibility of the line manager, liaising with and taking advice as necessary from the Information Governance Manager, to investigate such incidents and identify any learning points that must be implemented in order to prevent a recurrence.

Also see Procedure for dealing with Missing Records Appendix B

10 INFORMATION RISK

Threats to NHS data shall be appropriately identified and based upon robust risk assessments and risk management arrangements in line with the organisations risk management strategy and policy, and shall be managed and reviewed regularly to ensure:

- protection against unauthorised access or disclosure
- that the integrity and value of information is maintained
- that information is only available to authorised personnel as when it is required.

The organisation will ensure adequate audit provision, based upon robust risk management arrangements, ensuring the continuing effectiveness of NHS information security management arrangements.

In particular, the organisation will set out its commitment to create, maintain and manage the security of its key information assets (including its records) and other external information resources that it depends upon, and documents its principle activities in this respect.

Also see the Trust Risk Management Policy for more detailed guidance

11 RESEARCH GOVERNANCE

Any research, as opposed to audit, undertaken using patient records must first be approved by a Local Research Ethics Committee and given approval by the organisation as part of the Research Governance Framework. For advice on your proposed project and requests for information from other organisations, please contact the organisations Clinical Effectiveness lead.

12 DUE DILIGENCE

Consultation will take place, involving staff across all protected characteristics together with information generated from the Patient Satisfaction Questionnaires in relation to their perceptions on how we manage and handle their information.

There is no likely adverse impact on staff or service users from this policy as all information should be managed and handled within clear guidance. This policy sets out what these standards are and the steps to ensure these are met.

Benefits to the organisation in regard to savings include increased staff awareness of their legal and statutory duties in relation to the handling and management of information.

13 TRAINING

There is a need for training identified within this policy. In accordance with the classification of training outlined in the Trust Human Resources & Organisational Development Strategy this training has been identified as mandatory and forms part of the Information Governance training.

The course directory e- source link below will identify: who the training applies to, delivery method, the update frequency, learning outcomes and a list of available dates to access the training.

All staff in the organisation will be made aware of their responsibilities for record-keeping and record management through generic and specific training programmes and guidance. It must take full account of this policy.

Staff need to have an understanding of:

- what they should record;
- why they are recording it and how it will be used;
- how to validate the information with the patient or against other records – so;
- staff are recording the correct data.

- how to update information and add in information from other sources
- the correction of errors – so staff know how to correct errors and how to report errors if they find them
- how information is shared
- how information is to be kept secure

Training in records management will be included in mandatory induction training for all staff, and refresher sessions made available to staff as and when needed.

Staff with specialist records responsibilities will receive appropriate training and will be kept up to date with new processes and procedures.

14 EQUALITY IMPACT ASSESSMENT

All relevant persons are required to comply with this document and must demonstrate sensitivity and competence in relation to the nine protected characteristics as defined by the Equality Act 2010. In addition, the Trust has identified Learning Disabilities as an additional tenth protected characteristic. If you, or any other groups, believe you are disadvantaged by anything contained in this document please contact the Equality and Diversity Lead who will then actively respond to the enquiry.

15 MONITORING COMPLIANCE AND EFFECTIVENESS

Overall monitoring of compliance with this policy will be the responsibility of the Caldicott and Information Governance Group who receive quarterly reports from the Information Governance Manager. The Caldicott and Information Governance Group will provide a six monthly progress report to the Integrated Governance Committee.

In addition, the Clinical Governance Group will be responsible for the monitoring of compliance with clinical records where held in paper form and report issues to the appropriate Best Practice Group who will report significant issues to the Caldicott and Information Governance Group.

16 PROCESS FOR MONITORING COMPLIANCE

Overall monitoring will be the responsibility of the Caldicott and Information Governance Group who receive quarterly reports, including monitoring, from the Information Governance Manager and, where required, the Trust Best Practice Groups.

Monitoring will be by:

Annual clinical audits as per the Trustwide Clinical Audit Plan, focusing on the following areas:

- Community Hospitals
- Minor Injury Units (MIUs)
- Community Specialist Services

- Mental Health Inpatient Wards
- Mental Health Community based patients
- Information Governance Toolkit requirement 10-404
- Random sampling of staff by questionnaire
- internal audits
- external auditor investigations and reports
- complaints monitoring
- incident reporting and monitoring

Shortfalls identified will be discussed at the Caldicott and Information Governance Group and Action Plan(s) devised. The Caldicott and Information Governance Group will provide a six monthly progress report to the Integrated Governance Committee using the Reporting Template.

The Trust Best Practice Groups will, as required, provide reports to the Clinical Governance Group using the Governance Reporting Template.

Lessons Learnt will be noted by the Caldicott and Information Governance Group within the report to the Integrated Governance Committee.

Results of clinical audits will be circulated to all staff within the Trust Somerset Partnership Improving Clinical Effectiveness (SPICE) Newsletter, and published on the intranet.

17 COUNTER FRAUD

The Trust is committed to the NHS Protect Counter Fraud Policy – to reduce fraud in the NHS to a minimum, keep it at that level and put funds stolen by fraud back into patient care. Therefore, consideration has been given to the inclusion of guidance with regard to the potential for fraud and corruption to occur and what action should be taken in such circumstances during the development of this procedural document.

18 RELEVANT CARE QUALITY COMMISSION (CQC) REGISTRATION STANDARDS

18.1 Under the **Health and Social Care Act 2008 (Regulated Activities) Regulations 2014 (Part 3), the fundamental standards** which inform this procedural document, are set out in the following regulations:

Regulation 9:	Person-centred care
Regulation 10:	Dignity and respect
Regulation 11:	Need for consent
Regulation 12:	Safe care and treatment
Regulation 13:	Safeguarding service users from abuse and improper treatment
Regulation 15:	Premises and equipment
Regulation 17:	Good governance
Regulation 18:	Staffing
Regulation 20:	Duty of candour
Regulation 20A:	Requirement as to display of performance assessments.

18.2 Under the **CQC (Registration) Regulations 2009 (Part 4)** the requirements which inform this procedural document are set out in the following regulations:

Regulation 18: Notification of other incidents

18.3 Detailed guidance on meeting the requirements can be found at http://www.cqc.org.uk/sites/default/files/20150311%20Guidance%20for%20providers%20on%20meeting%20the%20regulations%20FINAL%20FOR%20PUBLISHING.pdf

Relevant National Requirements

- NHS Records Management
- Information Governance Toolkit
- Public Records Act 1958
- Freedom of Information Act 2000

19 REFERENCES, ACKNOWLEDGEMENTS AND ASSOCIATED DOCUMENTS

- Department of Health. (April 2007). Information Security Management: NHS Code of Practice. London: Department of Health. Available at: www.dh.gov.uk
- Department of Health. (2006). Records Management: NHS Code Of Practice Part 1 and Part 2. London: Department of Health. Available at: www.dh.gov.uk
- NHS Connecting for Health. (2006). Information Governance Toolkit. Available at: www.connectingforhealth.nhs.uk
- Nursing and Midwifery Council. (2009). Guidelines for Records and Record Keeping. London: Nursing and Midwifery Council.
- Data Protection Act 1998. London: The Stationery Office. Freedom of Information Act 2000. London: The Stationery Office.
- NHS Connecting for Health Information Governance Toolkit 2015 (Version 13)
- Department of Health Records Management: NHS Code Of Practice (2009)
- HMSO Data Protection Act 1998 (1998)
- General Medical Council (2014) Keeping Records
- Health and Care Professions Council (2008) Standards of Conduct, Performance and Ethics:21

Cross reference to other procedural documents

- Confidentiality and Data Protection Policy
- DATIX Risk Register Guidance
- Development & Management of Procedural Documents
- Freedom of Information Policy
- Information Governance Policy
- Information Security Policy
- Risk Management Policy and Procedures
- Consent and Capacity for Treatment Policy

20 APPENDICES

For the avoidance of any doubt the appendices in this policy are to constitute part of the body of this policy and shall be treated as such.

Appendix A – Supporting Documentation

Appendix B – Dealing with Lost Records procedure

Appendix A – Supporting Documentation

To support the requirements of Sections 6, 7 & 8 of this policy the Information Governance Team will issue local protocols, procedures. These documents will be referenced here along with other relevant Trust policies, protocols, procedures.

A6.1 Record Creation

Document Title	Audience	Publication Date	Review Date
Register a Patient on RiO	All Staff	September 2015	
Record the consent to share information	All Staff	September 2015	
Creation of paper based record system	All Staff	September 2015	
Creation of Corporate Records system	All Staff	September 2015	
Creation of Logical Record Folders	All Staff	September 2015	
Creation of Electronic System Additional Requirements	SIRO/ IAO / IAA	September 2015	

A6.2 Record Retention

Document Title	Audience	Publication Date	Review Date
Guide to Record Retention.pdf	All Staff		
Record retention periods by record type	All Staff		
Department of Health Records Management (detailed)	SIRO / IAO / IAA		
Department of Health Retention Scheduled (Detailed)	SIRO / IAO / IAA		

A6.3 Record Maintenance

Document Title	Audience	Publication Date	Review Date
Scanning documents to RiO	All Staff		
Maintaining the record Data Protection Act requirements	All Staff		

A6.4 Record Use

Document Title	Audience	Publication Date	Review Date
Transporting of Patient Records	All Staff		
Correspondence with patients and capacity issues	All Staff		
Subject Access Requests	All Staff		
Access to patient or staff records procedure	All Staff		
Access to deceased patients procedure	All Staff		
Missing Record Procedure	All Staff		
Medical Reports Procedure	All Staff		

A6.5 Record Disposal

Document Title	Audience	Publication Date	Review Date

Appendix B

Dealing with Lost Records procedure

MISSING RECORD PROCEDURE

The Missing Record Procedure had been developed to implement effective tracking systems for health and personnel records.

This supports processes to ensure that health records and personnel records are made available when required. A record is kept of all missing records and the reason for non-availability is recorded.

A "**missing record**" is a record that is unavailable within **5 working days** of the first attempt to access the record when required for clinical or administrative use; an out-patient appointment; admission or other service user contact; complaints, legal investigations; subject access requests; incident investigations.

When this occurs the following steps must be undertaken:

1. The member of staff should report this to his/her supervisor/ line manager as soon as possible before the service user is due to attend or record required.

2. The supervisor / line manager should ensure that a thorough search is undertaken, using tracking and service contact history, including initiating a search at the base where the record should be kept.

3. An electronic incident form must also be completed at this stage as per the Incident Reporting Policy.

The Information Governance & Records Manager may instigate the need to complete an IG SIRI investigation, depending on the circumstances of the loss e.g. a number of records are identified as missing or a complaint to the Information Commissioner (ICO) or litigation case may occur.

4. On receipt of an incident form relating to missing records, the Information Governance & Records Manager will issue a Missing Record Log and procedure to the department and will discuss with the lead clinician if it is appropriate to inform the service user or carer in the case of health records. Further advice can be sought from the Information Governance & Records Manager.

5. The Information Governance & Records Manager grades the incident according to the checklist guidance for Reporting, Managing and Investigating Information Governance Serious Incidents requiring Investigation (SIRI). If the incident level is graded a 2 or above then the incident will be reported to the ICO and DH automatically via the IG Incident Reporting Tool.

If the incidents are reported to the ICO as above then the following should also be notified: Caldicott Guardian, SIRO, Service Director and Governance Lead.

6. The missing record or volume should be highlighted as missing (adding a comment to this effect on electronic tracking system) and a temporary record should be created, clearly marked as a temporary record, populated with all relevant

information available for that service user / member of staff. A temporary record should be set up and tracked on the relevant systems (electronic or manual) or noted that a temporary record has been created.

7. When the original record is located the missing record log should be updated with the details of when/ how the original was located, and the temporary and original record should be merged

8. The supervisor / manager should send a copy of the missing records log to the Information Governance Manager

9. The records management service will be authorised to monitor all departments' compliance with this procedure and identify any actions to be undertaken

10. The Caldicott & Information Governance Group is responsible for implementing any action plans arising from non-compliance to the Records Keeping and Records Management Policy in respect of missing or lost records.

Lost / destroyed records

When a set of records has been missing for 6 months, it is reasonable to assume that the original set of records has been lost.

The missing record log must then be returned to the Information Governance & Records Manager. This is kept with the original incident form.

Found Records

When the original records are located the following procedure should be followed:

1. Complete the missing record log to indicate that the original records have been located

2. For health records inform the lead clinician. If the service user / carer had been previously informed that the records were missing the lead clinician will need to inform the service user / carer that the records had been found.

3. Merge the temporary folder with the original set of records

4. For mental health hospital records if the original records are found the temporary patient document on the electronic tracking system should be marked as inactive and end dated as at the date of the physical merge into the case notes that have been found. Remove the comment on these notes on the electronic tracking system

5. Remove the indicator on the electronic tracking system showing that a temporary file or duplicate record is in circulation

6. Update the electronic tracking system with the location of the merged records

7. Inform the Information Governance & Records Manager