140929

South Central Ambulance Service
NHS Foundation Trust

CORPORATE POLICY & PROCEDURE NO. 18

LIFECYCLE POLICY

June 2018

DOCUMENT INFORMATION	
Author: Barbara Sansom, Information Governance Manager	**Consultation & Approval** Staff Consultation 21 days Audit Committee: October 2018 Board Ratification: N/A
Equality Impact Assessment	April 2018 - Stage 1 Assessment undertaken – no issues identified
Data Protection Impact Assessment:	April 2018 – Initial/High Level Assessment undertaken – no issues identified
Notification of Policy Release:	All Recipient email Intranet Website
Date of Issue:	June 2018
Next Review:	June 2021
Version:	**6.1** – summary record retention schedule added (Appendix 1) **6.0** – content changes to reflect General Data Protection Regulations (GDPR) & Data Protection Act (DPA) 2018 5.1 no content changes – period extended to 30th June 2018 to allow for review under new DPA / GDPR rules 5 (no content changes)

CONTENTS

1 Introduction

1.1 This policy applies to all information that is recorded and held by the Trust. It refers to both health and corporate records held in any format.

1.2 For the purposes of this Policy, a record is defined as anything, which contains information (paper, electronic, tape, video etc), which has been created or gathered as a result of any aspect of the work of NHS employees - including consultants, agency or casual staff.

1.3 The Public Record Office has published a Record Management Standard which states that "*A systematic and planned approach to management of records within an organisation, from the moment they are created to their ultimate disposal, ensures that the organisation can control both the quality and the quantity of the information in a manner that effectively serves its needs, those of the government and of the citizen; and it can dispose of the information efficiently when it is no longer required*"

1.4 The Department of Health has published the Records Management: NHS Code of Practice which the South Central Ambulance Service NHS Foundation Trust has endorsed as best practice in the management of records.

1.5 All NHS records are public records under the terms of the Public Records Act 1967, which confers a statutory duty on the Trust for their safekeeping and eventual disposal.

1.6 The Trust's records are a valuable resource because of the information they contain, supporting operations, providing evidence of decision making and influencing policy formation.

1.7 Information is essential to the delivery of high quality evidenced based health-care on a day to day basis and effective records management supports:

- Patient care and continuity of care
- Day to day business which underpins delivery of care
- Evidence based clinical practice
- Sound administrative and managerial decision making
- Meeting legal requirements include data subject access requests

Records will be managed so that they are:

- available when needed
- accessible
- easily interpretable
- reliable
- secure
- retained and disposed of appropriately

2 Aim

2.1 This Policy identifies the actions required to ensure that records of all types (administrative as well as Health) are properly controlled, readily accessible and available for use, and eventually archived or otherwise appropriately disposed of.

2.2 It informs staff of the requirements and expectations in relation to records management.

2.3 It protects the Trust as an employer and ensures we comply with the relevant legislation and codes of practice.

3 Scope

This policy applies to:

- Anyone processing information on behalf of SCAS, including all staff employed by the Trust, contracted third parties, agency staff, students, trainees, secondees, locum staff, staff on temporary placements, volunteers. It applies to Non-Executive Directors and any individuals not directly employed by the Trust such as community responders or volunteers
- All information (manual and electronic), information systems, networks, application and SCAS locations
- All business functions within SCAS
- All organisations providing a service on behalf of SCAS
- All services commissioned by SCAS
- Anyone having access to the SCAS IT network

4 Responsibilities

Information governance roles and responsibilities are detailed in the Trusts information governance policy. Responsibilities specific to this policy are outlined below:

4.1 Board level responsibility for Records Management and management of information lies with the Director of Finance. The Trust has an Information Governance Manager who is responsible for the implementation of the Information Lifecycle Strategy relating to this policy and reports to the Director of Finance via the Associate Director of IM&T.

4.2 The Trust has a Board level Caldicott Guardian who works closely with the Information Governance Manager on issues of Clinical record keeping

4.3 Senior managers in each directorate have lead responsibility and are accountable for the quality of records management.

4.4 Line managers must ensure that staff are adequately trained and apply the appropriate guidelines.

4.5 Every member of staff is responsible for any records they create, or use. This responsibility is established at, and defined by the law. Furthermore, as an employee of the NHS, any records, which you create, are public records and must be shared in accordance with Freedom of Information Act and Data Protection Act.

5 Records Management

5.1 Records Creation

5.1.1 The content of a record will primarily be determined by the purpose for which it is being created, for example a personnel file will contain information about an employee relating to things like employment history and training; a patient file will contain information about treatment.

5.1.2 Record keeping is a tool of professional practice and one, which should help the operational process. It is not separate from the process and it is not an optional extra to be fitted in.

5.1.3 Records of business activity should be complete enough to:

- facilitate an audit or examination of the business by anyone so authorised
- protect the legal and other rights of the Trust, its clients and any other person affected by its actions
- provide authenticity of the records so that the evidence derived from them is shown to be credible and authoritative.

5.1.4 Records should be:-

- factual, consistent and accurate,
- written in plain English
- written as soon as possible after an event has occurred, providing current information,
- written clearly and in such a way that the text cannot be erased,
- written in such a way that any alterations or additions are dated, timed and signed in such a way that the original entry can still be read clearly,
- accurately dated, timed and signed with the signature printed alongside the first entry,
- not include abbreviations (unless officially accepted e.g. Clinical or Medical), jargon, meaningless phrases, irrelevant speculation and offensive subjective statements,
- readable on any photocopies,
- written in black pen (not ink, as ink will run if it comes into contact with a liquid) and on white paper, (although other coloured pens and paper can be used providing the combination of pen and paper produces a legible and permanent record- blue ink produces very poor reproduction).
- do not include the use of correction fluid.

5.2 Records Maintenance and Storage

5.2.1 Records should be created and stored in line with the Trust's procedure for electronic and paper filing systems. Records should be stored to comply with health and safety standards and should not be stored where they could be damaged by fire or water.

5.2.2 Records that are used for operational purposes should be stored in such a manner that they are easily retrievable.

5.2.3 When records are no longer required for operational purposes, they may be sent to a secure off-site storage facility, but wherever possible transferred to an electronic format through a scanning process.

5.2.4 The criteria for deciding when a record should be sent off-site will take into account amongst other things the last time the record was required for operational purposes, on-site storage availability, and the likelihood of the record being required for operational purposes again.

5.2.5 In the secure storage area, records will be filed in a way that facilitates their location and retrieval, and the area will be kept clean and tidy.

5.2.6 The Information Governance Manager will control requests for the transfer and return of records through colleagues within each Directorate.

5.2.7 All records sent off site are subject to contractual arrangements that must comply with relevant legislation and guidance.

5.2.8 Electronic records may be archived within an information system if such functionality has been verified to meet information security standards.

5.3 Retention and Destruction / Disposal of Records

5.3.1 For the purpose of this document Destruction is referred to as an irreversible act. Disposal could be the transfer of records form one media to another e.g. paper records to electronic storage device or transfer of records from one organisation to another.

5.3.2 The length of the retention period depends upon the type of record and its importance to the Trust. The Department of Health provides 'guidance' in the Records Management: NHS Code of Practice for Health and Social Care, which sets out the minimum recommended retention periods for both clinical and administrative records. This period of time will be calculated from the end of the calendar or accounting year following the last entry in the record (e.g. manual file, computer record). See Appendix 1 for a summary of retention periods

5.3.3 There is a legal requirement under the GDPR and DPA 2018 that personal information should not be kept for longer than is necessary – the NHS interpretation of this requirement is that the retention periods specified in the relevant circulars are normally deemed to be the 'necessary' time period. Therefore provided the timescales detailed in the relevant circular are complied with, there should also be compliance with the data protection requirements. If it is decided that records may need to be kept for longer than specified in the relevant circular this may need to be justified as it may breach the requirements of the GDPR and DPA 2018.

5.3.4 The decision to destroy records will be taken by the Senior Manager within the Directorate only after the minimum retention period has been exceeded, and where s/he is satisfied that no useful purpose can be served by further retention and after seeking advice from the Information Governance Manager. Within the Trust these nominated managers are:

Directorate	Senior Manager
Finance	Director of Finance
Medical Records	Director of Patient Care
Policy Information	Company Secretary
Human Resources	HR Director
Chief Executives / Non Executives Office	Company Secretary
Operational and Performance Records	Chief Operating Officer
Information Technology & Information Governance	Associate Director of Information Management and Technology

5.3.5 The normal method of destruction used within the NHS is one of the following:

- Shredding
- Pulping
- Incineration

5.3.6 Destruction of IT equipment should be undertaken by approved contractors or specialists in the destruction of IT hardware.

5.3.7 All 'off site' destruction should be accompanied by 'proof of destruction' in the form of a certificate. This should be kept as an audit trail.

Note: If a record due for destruction is known to be the subject of a request for information, under Freedom of Information or Data Protection, destruction should be delayed until disclosure has taken place or, if the Trust has decided not to disclose the information, until the complaint and appeal provisions of the Freedom of Information Act have been exhausted.

5.3.8 It is the responsibility of The Trust to satisfy itself that records are destroyed in a way that safeguard against accidental loss or disclosure of contents

Refer to the Records Management: NHS Code of Practice for Health and Social Care **for guidance on retention periods and Appendix 1 for a summary of retention periods**

6 Access to records

6.1 Under the GDPR and DPA 2018, individuals have rights to access personal data held about them. Typically, this will involve supplying an individual with access to, or a copy of their record when asked to do so. The Access to Health Records Act 1990 applies to requests for access or a copy of records of deceased patients by their personal representatives or those with an interest in the deceased's estate.

6.2 Formal requests for access should be made in writing to the Trust Information Governance Manager. Access to a personal record will be facilitated within one month of receipt of a bona fide request.

6.3 This should be read alongside the Trust Data Protection Policy and guidance on data subject rights.

7 References

7.1 Key Legislation

- Public Records Act
- General Data Protection Regulation (GDPR)
- Data Protection Act 2018 (DPA 2018)
- Freedom of Information Act (FOIA) 2000
- Access to Health Records Act 1990
- Human Rights Act 1998

8 Linked Policies

- Lifecycle Strategy
- Data Protection Policy
- Information Governance Policy
- Confidentiality Policy
- Freedom of Information Policy
- Freedom of Information Publication Scheme
- IM & T Policies & Procedures

9 Equality Statement

9.1 The Trust is committed to promoting positive measures that eliminate all forms of unlawful or unfair discrimination on the grounds of age, marital status, disability, race, nationality, gender, religion, sexual orientation, gender reassignment, ethnic or national origin, beliefs, domestic circumstances, social and employment status, political affiliation or trade union membership, HIV status or any other basis not justified by law or relevant to the requirements of the post.

9.2 By committing to a policy encouraging equality of opportunity and diversity, the Trust values differences between members of the community and within its existing workforce, and actively seeks to benefit from their differing skills, knowledge, and experiences in order to provide an exemplary healthcare service. The Trust is committed to promoting equality and diversity best practice both within the workforce and in any other area where it has influence.

9.3 The Trust will therefore take every possible step to ensure that this procedure is applied fairly to all employees regardless of race, ethnic or national origin, colour or nationality; gender (including marital status); age; disability; sexual orientation; religion or belief; length of service, whether full or part-time or employed under a permanent or a fixed-term contract or any other irrelevant factor.

9.4 Where there are barriers to understanding e.g. an employee has difficulty in reading or writing or where English is not their first language additional support will be put in place wherever necessary to ensure that the process to be followed is understood and that the employee is not disadvantaged at any stage in the procedure. Further information on the support available can be sought from the Human Resource Department.

10 Monitoring & Review

10.1 The Information Governance Steering Group will be responsible for the monitoring the policy and its supporting processes and documentation, reporting regularly to the Trust IM&T Control Board.

10.2 This policy will be in place for three years. Any changes to legislation, statute or NHS operational guidance which requires a change of policy within the three year period will be considered by the Information Governance Steering Group.

10.3 In the event of significant failure of this policy, then the group will approve temporary changes prior to formal review.

10.4 The policy will next be reviewed in June 2021.

Appendix 1

Summary – Record Retention Periods

Record Type	Retention Start	Retention Period	Action at end of Retention Period
Adult Health Records	Discharge or patient last seen	8 years	Review & securely destroy
Child Health Records	Discharge or patient last seen	Child's 26th birthday	Review & securely destroy
Clinical Audit	Creation	5 years	Review & securely destroy
Destruction certificates / electronic metadata destruction stub	Destruction of record or information	20 years	Review and either transfer to Place of Deposit or securely destroy
Telephony systems services (voice recordings)	Creation	To be agreed by Patient Safety Group	
Board Meetings	Creation	20 years	Transfer to Place of Deposit
Serious Incidents	Date of incident	20 years	Review and consider transfer to a Place of Deposit
Incidents (non-serious)	Date of incident	10 years	Review and if no longer required destroy securely
Patient Advice & Liaison records	Close of financial year	10 years	Review & securely destroy
Intranet site	Creation	6 years	Review and consider transfer to a Place of Deposit
Press releases & important internal communications	Creation	6 years	Review and consider transfer to a Place of Deposit
Website	Creation	6 years	Review and consider transfer to a Place of Deposit
Duty roster	Close of financial year	6 years	Review and if no longer required destroy securely
Staff occupational health records	Staff member leaves	Until 75th birthday or 6 years after staff member leaves	Review and if no longer required destroy securely
Staff record	Staff member leaves	Until 75th birthday	May be destroyed 6 years after staff member leaves is a summary is made

Record Type	Retention Start	Retention Period	Action at end of Retention Period
Staff Record Summary	6 years after staff member leaves	Until 5th birthday	Transfer to Place of Deposit or destroy
Timesheets	Creation	2 years	Review and if no longer required destroy securely
Contracts	End of contract	6, 15 or 11 years (see full retention schedule)	Review and if no longer required destroy securely
Tenders	End of contract	6 years	Review and if no longer required destroy securely
CCTV		Dependent on purpose – see ICO guidance	
Complaints	Closure of incident	10 years	Review and if no longer required destroy securely
Freedom of Information (FOI) requests	Closure of request	3 years or 6 years from closure of any appeal	Review and if no longer required destroy securely
Litigation records	Closure of case	10 years	Review and consider transfer to a Place of Deposit
Subject Access Requests (SARs)	Closure of request	3 years or 6 years from closure of any appeal	Review and if no longer required destroy securely