South Central Ambulance Service
NHS Foundation Trust

CORPORATE POLICY & PROCEDURE NO. 7

INFORMATION GOVERNANCE POLICY

June 2018

DOCUMENT INFORMATION	
Author: Barbara Sansom, Information Governance Manager	**Consultation & Approval** Staff Consultation Audit Committee: January 2015 Board Ratification: N/A
Equality Impact Assessment	December 2014 – Stage 1 Assessment undertaken – no issues identified
Data Protection Impact Assessment:	Initial/High Level Assessment undertaken – no issues identified
Notification of Policy Release:	All Recipient email Staff Notice Boards Intranet
Date of Issue:	June 2018
Next Review:	June 2021
Version:	7.0 -– content changes to reflect General Data Protection Regulations (GDPR) & Data Protection Act (DPA) 2018

Contents

1. Introduction 3
2. Principles 3
3. Scope 5
4. Roles and Responsibilities 5
5. Linked Trust Documents 7
6. Equality Statement 7
7. Monitoring & Review 7

1. Introduction

Information is a vital asset, both in terms of the clinical management of individual patients and the efficient management of services and resources. It plays a key part in clinical governance, service planning and performance management.

It is therefore of paramount importance to ensure that information is efficiently managed, and that appropriate policies, procedures and management accountability and structures provide a robust governance framework for information management.

2. Principles

The South Central Ambulance Service NHS Foundation Trust *(The Trust)* recognises the need for an appropriate balance between openness and confidentiality in the management and use of information. The Trust fully supports the principles of corporate governance and recognises its public accountability, but equally places importance on the confidentiality of, and the security arrangements to safeguard, both personal information about patients and staff and commercially sensitive information. The Trust also recognises the need to share patient information with other health and social care organisations and other agencies in a controlled manner consistent with the interests of the patient and, in some circumstances, the public interest.

The Trust believes that accurate, timely and relevant information is essential to deliver the highest quality health care. As such it is the responsibility of all clinicians and managers to ensure and promote the quality of information and to actively use information in decision making processes.

There are 4 key interlinked strands to the information governance policy:

- Openness
- Legal compliance
- Information security
- Quality assurance

2.1. **Openness**

- Non-confidential information on the Trust and its services should be available to the public through a variety of media.
- The Trust will establish and maintain policies to ensure compliance with the Freedom of Information Act.
- The Trust will undertake or commission annual assessments and audits of its policies and arrangements for openness.
- Patients should have ready access to information relating to their own health care, their options for treatment and their rights as patients.
- The Trust will have clear procedures and arrangements for liaison with the press and broadcasting media.
- The Trust will have clear procedures and arrangements for handling queries from patients and the public.

2.2. **Legal Compliance**

- The Trust regards all identifiable personal information relating to patients as confidential.
- The Trust will undertake or commission annual assessments and audits of its compliance with legal requirements
- The Trust regards all identifiable personal information relating to staff as confidential except where national policy on accountability and openness requires otherwise.
- The Trust will establish and maintain policies to ensure compliance with the General Data Protection Regulation (GDPR), Data Protection Act 2018 (DPA 2018), Human Rights Act and the common law of confidentiality.
- The Trust will establish and maintain policies for the controlled and appropriate sharing of patient information with other agencies, taking account of relevant legislation (e.g. Health and Social Care Act, Crime and Disorder Act, Children's Act and the Caldicott principles).

2.3. **Information Security**

- The Trust will establish and maintain policies for the effective and secure management of its information assets and resources.
- The Trust will undertake or commission annual assessments and audits of its information and IT security arrangements.
- The Trust will promote effective confidentiality and security practice to its staff through policies, procedures and training.
- The Trust will establish and maintain incident reporting procedures and will monitor and investigate all reported instances of actual or potential breaches of confidentiality and security.
- Utilise the Data Security and Protection Toolkit to identify information governance issues and address weakness through formal programmes of improvement.

2.4. **Information Quality Assurance**

- The Trust will establish and maintain policies and procedures for information quality assurance and the effective management of records.
- The Trust will undertake or commission annual assessments and audits of its information quality and records management arrangements.
- Managers are expected to take ownership of, and seek to improve, the quality of information within their services.
- Wherever possible, information quality should be assured at the point of collection.
- Data standards will be set through clear and consistent definition of data items, in accordance with national standards.
- The Trust will promote information quality and effective records management through policies, procedures/user manuals and training

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. Roles and Responsibilities

4.1. **The Chief Executive**

The Chief Executive is the Trust's Accountable Officer and has ultimate responsibility for meeting all statutory requirements, the governance of information and the implementation and compliance to this policy.

4.2. **Senior Information Risk Owner (SIRO)**

The SIRO for the Trust is the Director of Finance. The role is accountable for the overall development and maintenance of information governance within the Trust. The SIRO acts as champion for information risk on the Board of Directors and advises on the effectiveness of risk management across the Trust.

4.3. **Caldicott Guardian**

The Trust's Caldicott Guardian is the Executive Director of Patient Care.
The Caldicott Guardian:

- Serves in an advisory role and is the conscience of the organisation.
- Ensures the Trust meets the highest practical standards for processing patient information.
- Has overall responsibility for protecting the confidentiality of patient and service user information, enabling appropriate information sharing.

4.4. **Data Protection Officer (DPO)**

The role of the DPO is to inform and advise the Trust of obligations under the Data Protection Act 2018. The DPO reporting to the SIRO, will monitor compliance with the policies of the Trust in relation to the protection of personal data and will train staff and raise awareness as the need arises.
The DPO acts as the contact point for the Information Commissioner's Office on issues relating to processing.

4.5. **Information Governance Steering Group (IGSG)**

The Information Governance Steering Group will have membership drawn from all departments and

directorates to ensure that Information Governance is embedded within the organisational structure. The responsibilities of the IGSG include:

- monitoring the progress on the delivery of information governance strategy
- identifying information governance risks and mitigating to an acceptable level
- agreeing information governance policy

4.6. **The Information Governance Manager**

The Information Governance Manager is the lead senior manager responsible for ensuring the Trust complies with all aspects of information governance. The role is responsible for completing the Data Security and Protection Toolkit as well as setting and implementing appropriate policies and procedures.

4.7. **Information Asset Owners**

Information Asset Owners (IAOs) are directly accountable to the SIRO and must provide assurance that information risk is being managed effectively in respect of the information assets that they 'own'. They are responsible for identifying and documenting information flows in relation to their asset. They ensure that staff are aware of and comply with information governance and record management standards for the effective use of information assets.
IAOs may be assigned ownership of several assets within the Trust.

4.8. **Information Asset Administrators**

Information Asset Administrators are operational members of staff who understand and are familiar with information risks in their area or department. They implement the organisation's information risk policy and risk assessment process for those information assets they support and will provide assurance reports to the relevant Information Asset Owner as necessary.

4.9. **Information Governance Team**

The Information Governance Team provides support to the Information Governance Manager. The team ensures appropriate responses to all freedom of information and subject access requests within the allocated timescale, liaising with the appropriate professionals.

4.10. **Line Managers**

Line managers take responsibility for ensuring that the Information Governance Policy is implemented within their directorate, group or team.

4.11. **All Staff**

All SCAS staff have a personal responsibility to handle information in accordance with information governance policy and relevant legislation thus helping maintain the availability, effectiveness, security and confidentiality of information. They understand that failure to comply with information governance policy is treated seriously and can lead to disciplinary action.

4.11.1. All staff are mandated to complete annual data security awareness training.

5. Linked Trust Documents

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

6. Equality Statement

6.1. 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.

6.2. 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.

6.3. 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.

6.4. 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.

7. Monitoring & Review

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

7.1.1. The Data Protection Officer will assist monitor internal compliance and inform and advise on statutory obligations.

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

7.3. In the event of significant failure of this policy, the Information Governance Steering Group will approve temporary changes prior to formal review.

7.4. The policy will next be reviewed in June 2021.