South Central Ambulance Service
NHS Foundation Trust

CORPORATE POLICY & PROCEDURE NO. 6

INFORMATION GOVERNANCE STRATEGY
June 2018

DOCUMENT INFORMATION	
Author: Barbara Sansom, Information Governance Manager	**Consultation & Approval** Staff Consultation Audit Committee: 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
Date of Issue:	June 2018
Next Review:	June 2021
Version: 7.0	7.0 -– content changes to reflect General Data Protection Regulations (GDPR) & Data Protection Act (DPA) 2018

CONTENTS

1. Introduction

Information Governance is the term covering the information component of both Clinical Governance and Corporate Governance. It provides a framework for the management and handling of information and records in a confidential and secure manner to appropriate ethical and quality standards. In addition, it enables organisations to put in place procedures and processes that support the efficient location and retrieval of corporate records where and when needed, in particular to meet requests for information and assist compliance with contractual requirements.

The Data Security and Protection Toolkit is an online system which allows NHS organisations and partners to measure their performance against the National Data Guardian's 10 data security standards. It also allows members of the public to view participating organisations' assessments.

This strategy sets out the approach taken by the South Central Ambulance Service NHS Foundation Trust (referred to hereinafter as "SCAS" or "the Trust") to achieve a high standard of excellence of information governance and provide a robust framework for the future management of information.

2. Strategic Aims

The Trust's information governance aims are detailed below. Achievement of these aims will deliver a high standard of patient care as well as deliver essential compliance elements.

2.1. Policies and Processes

The Trust will establish, implement and maintain risk based information governance policies for the effective management of information. These policies will be integrated into its day to day operations. They will be compliant with current and relevant legislation, standards and codes of practice. They will be clear, accessible and aligned with Trust objectives.

2.2. Awareness

We will provide clear advice and guidance to ensure there is a high level of awareness of information governance policy and processes amongst staff and suppliers to reduce the risk of non-compliance. We will actively encourage a culture of ownership, personal responsibility and commitment to the high standard of excellence set by the Trust.

2.3. Monitoring & Assurance

Measures will be adopted to evaluate the practical operation and effectiveness of information governance policy and changes will be made where necessary.
The Trust's performance will be assessed using the Data Security and Protection Toolkit and action plans implemented to maintain and improve compliance.

2.4. Records and information management

We will ensure that effective processes are in place to manage records and information. Records of processing activity will be maintained to ensure that we know what information is held by the Trust, where it is stored and who it is shared with. This will enable us promptly respond to requests from data subjects and requests for information.

2.5. **Information security**

We will implement information security policies which take account of legislative requirements but which are appropriate, proportionate, measured and aligned to the Trust's risk appetite. We will support our staff by ensuring that information security policy and processes are clear and accessible, that help and guidance are available when needed, and by providing appropriate training to minimise the risk of human error.

2.6. **Collection and use of personal information**

We will promote transparency and openness about how we handle personal information providing assurance to patients and stakeholders that robust safeguards are in place to ensure that any personal and sensitive data held by the Trust will be managed and used responsibly, securely and fairly in full compliance with the relevant legislation.
Data Protection Impact Assessments will be carried out prior to the introduction of any new or changes to existing IT systems, business processes or initiatives which involve the collection and use of personal information.

3. Scope

This strategy is to be adhered to by:

- 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. Implementation

The Trust will ensure that the strategy is implemented through its Information Governance and other related Policies & Procedures over the short, medium and long term.
Information Governance covers a number of standards and requirements which will be adopted and implemented. These are:

- The Common Law Duty of Confidentiality and the Confidentiality: NHS Code of Practice which provides specific guidance on when information should be kept confidential;
- The General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA 2018) which establishes a framework of rights and duties which are designed to safeguard personal data;
- The Caldicott Principles which provide rules relating to the handling and protection of patient information and requires all NHS organisations to have a Caldicott Champion;
- The Freedom of Information Act 2000 which provides a public right of access to the information held by, and on behalf of, public authorities; and
- The Public Records Act 1958 and Records Management Code of Practice for Health and Social Care 2016 which details requirements relating to the retention and storage of records by public authorities.

- The Data Security and Protection Toolkit which is an online system which allows NHS organisations to assess themselves against the National Data Guardian's 10 data security standards will be used to measure and report compliance.

Staff will be supported by providing policy and processes that are clear and accessible. Help, guidance and awareness training appropriate to the needs of each individual will be provided when needed.

All policies, work programmes and action plans will be approved and monitored by the Information Governance Steering Group.

5. Roles and Responsibilities

5.1. **The Board of Directors**

The Trust Board has ultimate responsibility for Information Governance within the Trust, however it has devolved responsibility for monitoring the progress of this strategy and associated policies. The Information Governance Steering Group is accountable to the Audit Committee and to the Trust Board. This group has overall responsibility for overseeing the implementation of this strategy, the Information Governance policy and action plan. These will be subject to periodic review with progress being reported to the Board through the Audit Committee.

5.2. **The Chief Executive**

The Chief Executive is the Trust's Accountable Officer and has ultimate responsibility for Information Governance, ensuring that information risks are assessed and mitigated to an acceptable level.
The Accounting Officer is responsible for the Information Governance Assurance Statement that confirms the Trust meets the information governance standards in respect of data security set out in Department of Health guidance.

5.3. **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.

5.4. **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. The Caldicott Guardian has overall responsibility for protecting the confidentiality of patient and service user information and enabling appropriate information sharing.

5.5. **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 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.

5.6. **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

5.7. **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.

5.8. **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.

5.9. **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.

5.10. **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.

5.11. **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.

6. Linked Trust Documents

- Information Governance Policy
- Confidentiality Policy
- Freedom of Information Policy
- Freedom of Information Publication Scheme

- IM & T Policies & Procedures
- Data Protection Policy
- Lifecycle Policy
- Safe Haven Policy

7. Equality Statement

7.1. 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.

7.2. 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.

7.3. 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.

7.4. 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.

8. Monitoring & Review

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

8.2. This strategy 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.

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

8.4. The strategy will next be reviewed in June 2021.