NHS
South East Coast Ambulance Service
NHS Foundation Trust

# Information Governance Policy

## Contents

# 1 Introduction

1.1. South East Coast Ambulance Service NHS Foundation Trust (the Trust) recognises that information is a vital asset, both in terms of the clinical management of individual patients and the efficient management of services and organisational resources. It plays a key part in clinical governance, service planning and performance management.

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

1.3. 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 other information that is exempt from disclosure, such as that which is commercially sensitive.

1.4. The Trust also recognises the need to share patient information with other health organisations or agencies in a controlled manner consistent with a legal basis in the interests of the patient, and, in some circumstances, the public interest.

1.5. 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 use information appropriately and actively in decision making processes.

# 2 Aims and Objectives

2.1. The key aims of this policy are to ensure that robust information governance arrangements, as determined by law and best practice, are in place to support the:

2.1.1. Proactive use of information within the Trust, both for patient care and service management, this also includes staff information.

2.1.2. Controlled sharing of patient information with other NHS and partner organisations to support patient care.

2.1.3. Trust’s commitment to making non-confidential information widely available for the public in line with our responsibilities under the Freedom of Information Act 2000 (FOIA).

2.1.4. Confidentiality, security and quality of personal and other sensitive information.

2.1.5. Availability of relevant, accurate and up to date records when needed to support business and clinical needs.

# 3 Definitions

3.1. **Information Governance** is the term used to describe the framework that brings together the requirements, standards and best practice that apply to the handling / processing of information. It enables organisations and individuals to ensure that information is dealt with legally, securely, efficiently and effectively in order to deliver the best possible care.

# 4 Policy Statement

4.1. This policy reflects the Trust's continued commitment to managing its information governance responsibilities appropriately by balancing its public duty to promote a culture of openness and transparency with its obligation to safeguard the confidentiality of certain record types that are exempt from disclosure.

4.2. By implementing this policy, the Trust acknowledges its responsibility to comply with its legal obligations to ensure that sound information governance arrangements are embedded throughout the Trust.

# 5 Arrangements

5.1. There are four interlinked strands to our information governance policy:

- Openness
- Legal compliance
- Information security
- Quality assurance

5.2. **Openness**

5.2.1. **Non-confidential** information on the Trust and its services will be available to the public through a variety of media, including its internet-based Publication Scheme, in line with the NHS commitment to openness. The Trust will establish and maintain policies and procedures to ensure compliance with the Freedom of Information Act 2000.

5.2.2. The Trust will undertake or commission regular, normally annual, assessments and audits of its policies and arrangements for openness.

5.2.3. Patients may readily access information relating to their own health care, their options for treatment and their rights as patients. The Trust will ensure that it has Privacy Notices in place, with website information available that details how patients may access their personal information and raise specific queries or concerns relating to their health records or treatment.

5.2.4. Patients or their representatives may request access to their personal information in line with data protection legislation (known as a data subject access request). The Trust will ensure that it has a Privacy Notice in place with website information available.

5.2.5. Employees may request access to their personal information in line with data protection legislation (known as a data subject access request). The Trust will ensure that it has employee Privacy Notices in place with website information available.

5.2.6. The Trust will make reasonable adjustments for anyone who cannot access information via the Trust public website. For example, by printing and mailing notices / information in response to a telephone request.

5.2.7. The Trust will have clear procedures and arrangements for liaison with the press and broadcasting media.

5.2.8. The Trust will have clear procedures and arrangements for handling queries from patients and the public.

5.3. **Legal Compliance**

5.3.1. The Trust regards all identifiable personal information relating to patients as confidential.

5.3.2. The Trust regards all identifiable personal information relating to staff as confidential except where national policy on accountability and openness requires otherwise.

5.3.3. The Trust will establish and maintain policies to ensure compliance with the Freedom of Information Act 2000, Data Protection Act 2018 (including the UK General Data Protection Regulation), Human Rights Act 1998 and the Common Law Duty of Confidentiality.

5.3.4. The Trust will undertake or commission regular, normally annual, assessments and audits of its compliance with legal requirements.

5.3.5. The Trust will establish and maintain protocols for the controlled and appropriate sharing of patient information with other agencies,

taking account of relevant legislation (e.g. Crime and Disorder Act 1998, Protection of Children Act 1999, Health Service (Control of Patient Information) Regulations 2002, NHS Act 2006, Health and Social Care Act 2012, etc.).

### 5.4. Information Security

5.4.1. The Trust will establish and maintain policies for the effective and secure management of its information assets and resources.

5.4.2. The Trust will undertake or commission regular, normally annual, assessments and audits of its information and IT security arrangements / systems.

5.4.3. The Trust will promote effective confidentiality and security practice to its staff through policies, procedures and training.

5.4.4. The Trust will establish and maintain incident reporting procedures and will monitor, investigate and audit all reported instances of actual or potential breaches of confidentiality and security.

### 5.5. Quality Assurance

5.5.1. The Trust will establish and maintain policies and procedures for information quality assurance and the effective management of records.

5.5.2. The Trust will undertake or commission regular, normally annual, assessments and audits of its information quality and records' management arrangements.

5.5.3. Managers are expected to take ownership of, and seek to improve, the quality of information within their services.

5.5.4. Wherever possible, information quality will be assured at the point of collection.

5.5.5. Data standards will be set through clear and consistent definition of data items, in accordance with national standards.

5.5.6. The Trust will promote information quality and effective records management via its policies, procedures / user manuals and training.

## 6 Responsibilities

6.1. It is the role of the Information Governance Working Group (IGWG) to review the Trust's policy and for the Joint Partnership Forum (JPF) to approve the Trust's policy and strategy in respect of Information Governance, taking into account legal and NHS requirements.

6.2. The IGWG is also responsible for ensuring that sufficient resources are provided to support the requirements of the policy. The Group will approve the annual Information Governance work programme and receive regular progress reports.

6.3. The Chief Executive Officer has overall responsibility as the Accountable Officer for Corporate Governance and the Caldicott Guardian is responsible for matters relating to patient confidentiality.

6.4. The Chief Digital and Information Officer (CDIO) is the Trust's designated Senior Information Risk Owner (SIRO) and is the Executive champion for the Freedom of Information Act 2000 within the Trust.

6.5. The Head of Information Governance / DPO is responsible for working with colleagues to ensure that the information governance work programme is delivered and reviewed annually.

6.6. The IGWG, which escalates issues to the Executive Management Team, is responsible for overseeing day to day Information Governance issues, developing and maintaining policies, standards, procedures and guidance, coordinating the Information Governance work programme throughout the Trust and raising staff awareness of it.

6.7. The IGWG will nominate leads for each of the component initiatives within the Information Governance framework. In addition to their responsibilities as members of the IGWG, Information Governance leads are responsible for producing gap analyses against the Cyber Assessment Framework / Data Security & Protection Toolkit requirements; producing action and implementation plans to ensure continuous improvement.

6.8. Managers within the Trust are responsible for ensuring that this policy and its supporting standards and guidelines are built into local processes and that there is on-going compliance.

6.9. All staff, (whether permanent, temporary or contracted), and contractors are responsible for ensuring that they are aware of the requirements incumbent upon them and for ensuring that they comply with these on a day-to-day basis.

6.10. Staff working remotely are responsible for ensuring they aware of the procedures of secure access to Trust information while doing so, and that they abide by the Trust's Remote Access Policy.

# 7 Competence

7.1. All staff are required to complete Information Governance training as part of their induction on joining the Trust's employment and to

undertake Statutory and Mandatory training on an annual basis through completing the IG training modules within SECAmb. Non-contract staff and those on short or fixed term contracts will also receive appropriate induction.

7.2. The Trust will offer more specialised in-house training to those whose role indicates that this is required. The IGWG is expected to provide expertise in the application of the Data Protection legislation and will be able to provide advice and guidance. The Trust SIRO, Deputy SIRO, Caldicott Guardian, Deputy Caldicott Guardian, Head of Information Governance, Data Protection Officer (DPO) and Information Governance Manager or individuals whose job role requires it, will receive additional specialised training appropriate to their roles and the Trust's needs.

7.3. Generic training will include:

- Personal responsibilities / accountability;
- Confidentiality of personal information;
- Relevant Trust Policies and Procedures;
- Compliance with the Data Protection legislation;
- Compliance with Caldicott principles;
- Individuals' rights (access to information and compliance with the principles);
- General good practice guidelines covering cyber security and confidentiality;
- Awareness of managerial responsibility for Data Protection and contact points for all issues that may occur in the areas of security and confidentiality of personal information;
- A general overview of all Information Governance components;
- A brief overview of how the Data Protection and Freedom of Information Acts work, and their differences;
- How to report incidents / learning events;
- How the Trust manages Information Governance and who the main contacts are.

7.4. The Trust Learning and Development department maintains training completion records for all Trust employees. The IGWG monitors IG training completion statistics via regular update throughout each financial year.

# 8 Monitoring

8.1. The Head of Information Governance / Information Governance Manager will monitor compliance with the key strands contained within this policy and report any issues, risks or non-compliance to each IGWG meeting.

8.2. The IGWG will report issues to the Executive Management Team as appropriate, via the Trust SIRO who is the IGWG Chair. These reports will detail progress in implementing annual improvement plans and highlight risks and areas of non-compliance.

# 9 Audit and Review

9.1. The Head of Information Governance / Information Governance Manager will produce annual gap analyses, action and implementation plans based on the requirements and guidance in the web based Cyber Assessment Framework / Data Security & Protection Toolkit to facilitate continuous improvement. These will be reviewed by IGWG and reported to the Executive Management Team via the Trust SIRO.

9.2. The JPF will give final approval to this policy.

9.3. The IGWG will oversee the implementation of this policy.

9.4. The Trust's internal auditors will undertake annual audits of the evidence supplied by the Trust to support its compliance with the Cyber Assessment Framework / Data Security & Protection Toolkit requirements. The resultant audit report will be presented to the Audit Committee, which will monitor action plans to address any gaps in compliance.

9.5. All policies have their effectiveness audited by the responsible Management Group at regular intervals, and initially six months after a new policy is approved and disseminated.

9.6. Effectiveness will be reviewed using the tools set out in the Trust's Policy and Procedure for the Development and Management of Trust Policies and Procedures (also known as the Policy on Policies).

9.7. All changes made to this policy will go through the governance route for development and approval as set out in the Policy on Policies.

9.8. This policy will be reviewed every three years or sooner if new legislation, codes of practice or national standards are introduced.

# 10 Equality Impact Appraisal

10.1. The Trust believes in fairness and equality, and values diversity in its role as both a provider of services and as an employer. The Trust aims to provide accessible services that respect the needs of each individual and exclude no-one. It is committed to comply with the Human Rights Act and to meeting the Equality Act 2010, which identifies the following nine protected characteristics: Age, Disability, Race, Religion and Belief, Gender Reassignment, Sexual Orientation, Sex, Marriage and Civil Partnership and Pregnancy and Maternity.

10.2. Compliance with the Public Sector Equality Duty: If a contractor carries out functions of a public nature then for the duration of the contract, the contractor or supplier would itself be considered a public authority and have the duty to comply with the equalities duties when carrying out those function.