South East Coast Ambulance Service NHS
NHS Foundation Trust

Information Governance Policy

Version:	6.00
Approved by:	Senior Management Team
Date approved:	03/11/2017
Name of originator/ author:	Information Governance Manager
Date issued:	06/11/2017
Review due:	3 November 2019
Target audience:	All Staff
Replaces:	5.0

Document Control

Manager Responsible

Name:	Caroline Smart
Job Title:	Information Governance Manager
Directorate:	Quality & Safety

Committee/Working Group to approve	Senior Management Team	
Version No. 5.00	Final	Date: 12/03/2012
Version No. 6.00	Policy reviewed	Date: 03/11/2017

Draft/Evaluation/Approval (Insert stage of process)

Person/Committee	Comments	Version	Date
Senior Management Team	Policy reviewed	V6.00	03/11/2017
Joint Partnership Forum		V6.00	30/10/2017
RMCGC	Approved	V5.00	12/03/2012
IGWG	Recommended for approval	V4.01	23/02/2012
IG Lead	Audit and Review, and Associated Documents updated	V4.01	February 2012
RMCGC	Noted confirmation of changes	V4.0	02/02/2012
Corporate Records Administrator	Reformatted to reflect FT status and changes in roles following workforce review	V4.0	07/12/2011
RMCGC	Approved in Principle at September 2011 meeting provided updates made by 11/12/2011	V3.01	12/09/2011
RMCGSC	Approved	3.00	05/02/2009
IGWG	formatting	V2.2	05/02/2009
IGWG Members	Minor grammatical changes	V2.1	25/01/2009
Head of Information Governance	Inserted new sections 2,4,10 & 12, updated sections 5.2.3, 6 and 11.		Jan 2009
RMCGSC	Approved	V2.0	15/03/2007
Trust Board	Approved	V1.0	17/07/2006
5 person committee	Agreed	V0.1	14/06/2006

Circulation

Records Management Database	Date: 06/11/2017
Internal Stakeholders	
External Stakeholders	

Active from (30 days after above signature):	Date:

Review Due

Manager	Information Governance Manager	
Period	Every two years or sooner if new legislation, codes of practice or national standards are introduced	Date: March 2015
Period	Policy reviewed	Date: November 2017

Record Information

Security Access/Sensitivity	Public Domain
Publication Scheme	Yes
Where Held	Records Management database
Disposal Method and date:	Non sensitive: 3 years after replacement

Supports Standard(s)/KLOE

	NHS Litigation Authority (NHSLA)	**Care Quality Commission (CQC)**	**Auditors Local Evaluation (ALE)**	**IG Toolkit**	**Other**
Criteria/KLOE:				**105**	

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

1.4. 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;

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 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 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:

5.1.1. Openness

5.1.2. Legal compliance

5.1.3. Information security

5.1.4. 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 make leaflets available that detail how patients may access their personal information and raise specific queries or concerns relating to their health records or treatment.

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

5.2.5. 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 1998, 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. Health and Social Care Act 2003, Crime and Disorder Act 1998, Protection of Children Act 1999).

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.

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 and investigate 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 through policies, procedures/user manuals and training.

6 Responsibilities

6.1. It is the role of the Information Governance Working Group to review the Trusts policy and for the Senior Management Team to approve the Trust's policy and strategy in respect of Information Governance, taking into account legal and NHS requirements. The Senior Management Team is also responsible for ensuring that sufficient resources are provided to support the requirements of the policy. The Senior Management Team will approve the annual Information Governance work programme and receive regular progress reports.

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

6.3. The Director of Strategy and Business Development is the Trust's designated Senior Information Risk Owner and is the Executive champion for Freedom of Information Act 2000 within the Trust.

6.4. The Information Governance Manager is responsible for working with colleagues to ensure that the information governance work programme is delivered and reviewed annually.

6.5. The Information Governance Working Group (IGWG) which reports into 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. 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 Information Governance Toolkit requirements; producing action and implementation plans to ensure continuous improvement.

6.6. 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.

6.7. 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.

7 Competence

7.1. All staff will receive annual mandatory Information Governance training. Information Governance leads and Trust managers, or individuals whose job role requires it, will receive more specialised training appropriate to their and the Trust's needs.

8 Monitoring

8.1. Information Governance leads 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 to the Executive Management Team at each meeting. These reports will detail progress in implementing annual improvement plans and highlight risks and areas of non-compliance.

9 Audit and Review

9.1. Information Governance leads will produce annual gap analyses, action and implementation plans based on the requirements and guidance in the web based Information Governance Toolkit to facilitate continuous improvement. These will be reviewed by IGWG and reported to the Executive Management Team

9.2. The Senior Management Team 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 IG 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. 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 has undertaken an Equality Impact Appraisal to identify whether it is likely to have an adverse impact on any groups and has not identified any significant risks.

11 Associated Documentation

11.1. Information Governance Strategy

11.2. Freedom of Information Policy and Procedure

11.3. Publication Scheme Procedure

11.4. Data Protection Policy

11.5. Data Subject Access Request Policy and Procedure

11.6. Transmission and Secure Storage of Confidential Information (Safe Haven) Policy

11.7. Records Management Policy

11.8. Records Management: Retention and Disposal Guidance

11.9. Confidentiality Code of Conduct

11.10. Information Security and Risk Management Policy

11.11. Information Risk Management Procedure

11.12. Internet and E-mail Policy

11.13. Mobile Devices Policy

11.14. Network Security Policy

11.15. Communications Strategy

11.16. Patient Advice and Liaison Procedure

11.17. Incident Reporting and Investigation Manual

12 References

12.1. Data Protection Act 1998

12.2. Human Rights Act 1998

12.3. Freedom of Information Act 2000

12.4. Confidentiality: NHS Code of Practice

12.5. Records Management: NHS Code of Practice

12.6. Information Security Management: NHS Code of Practice

12.7. Caldicott Principles