NHS
Surrey Downs
Clinical Commissioning Group

Information Governance Policy

Policy ID	IG02
Version	1.1
Owner	Justin Dix, Governing Body Secretary
Approving Committee	Information Governance Steering Group
Date agreed	27th January 2015
Next review date:	27th January 2017

Improving care together across Surrey Downs

Summary

This Policy outlines the CCG's approach to management of information handling including accountability and reporting arrangement. The policy sets out rules on how service-user and staff information must be used and shared.

Version History

Version	Review Date	Name of Reviewer	Ratification Process	Notes
0.1	27/11/2013	NHS South CSU IG Team	Final	Approved by Executive Committee
1.0	03/12/2014	NHS South East CSU IG Team	Draft	Complete revision to incorporate NHS South East IG Team guidance.
1.1	27/01/2015	NHS South East CSU IG Team	Final	Approved by Executive Committee
Contributors		Governing Body Secretary, Head of Planning & Performance and, South East CSU Information Governance Principle Associate.		
Audience		All CCG officers, Governing Body members and staff (which includes temporary staff, contractors and seconded staff) and CCG members in their capacity as commissioners.		

Equality Statement

Surrey Downs Clinical Commissioning Group (Surrey Downs CCG) aims to design and implement services, policies and measures that meet the diverse needs of our service, population and workforce, ensuring that none are placed at a disadvantage over others. It takes into account the Human Rights Act 1998 and promotes equal opportunities for all. This document has been assessed to ensure that no-one receives less favourable treatment on grounds of their gender, sexual orientation, marital status, race, religion, age, ethnic origin, nationality, or disability.

Members of staff, volunteers or members of the public may request assistance with this policy if they have particular needs. If the person requesting has language difficulties and difficulty in understanding this policy, the use of an interpreter will be considered.

Surrey Downs CCG embraces the four staff pledges in the NHS Constitution. This policy is consistent with these pledges.

Equality Analysis

This policy has been subject to an Equality Analysis, the outcome of which is recorded below.

1. Does the document/guidance affect one group less or more favourably than another on the basis of:			
	□ Race	Yes, No or N/A	Comments
	□ Ethnic origins (including gypsies and travellers)	No	
	□ Nationality	No	
	□ Gender	No	
	□ Culture	No	
	□ Religion or belief	No	
	□ Sexual orientation including lesbian, gay and bisexual people	No	
	□ Age	No	
	□ Disability - learning disabilities, physical disability, sensory impairment and mental health problems	No	
2	Is there any evidence that some groups are affected differently?	No	
3	If you have identified potential discrimination, are there any exceptions valid, legal and/or justifiable?	No	
4	Is the impact of the document/guidance likely to be negative?	N/A	
5	If so, can the impact be avoided?	N/A	
6	What alternative is there to achieving the document/guidance without the impact?	N/A	
7	Can we reduce the impact by taking different action?	N/A	

1. Introduction

1.1. Information is a vital asset. It plays a key part in ensuring the efficient management of service planning, resources and performance management.

1.2. 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.

1.3. Information Governance (IG) looks at the way the NHS handles information about patients, staff, contractors and the healthcare provided, with particular consideration of personal and sensitive information. Without access to information it would be impossible to provide quality healthcare. A robust governance framework needs to be in place to manage this vital asset, providing a consistent way to deal with the many different information handling requirements including:

- Information Governance Management
- Clinical Information assurance for Safe Patient Care
- Confidentiality and Data Protection assurance
- Corporate Information assurance
- Information Security assurance
- Secondary Use assurance

1.4. The aims of this document are to maximise the value of organisational assets by ensuring that information is:

- **H**eld securely and confidentially;
- **O**btained fairly and efficiently;
- **R**ecorded accurately and reliably;
- **U**sed effectively and ethically;
- **S**hared appropriately and lawfully

2. Scope and Definitions

2.1. The CCG recognises the need for an appropriate balance between openness and confidentiality in the management and use of information. The CCG 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 and commercially sensitive information. The CCG also recognises the need to share information in a controlled manner.

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

2.3. There are 4 key interlinked strands to the Information Governance Policy:

- Openness
- Legal compliance
- Information security
- Quality assurance

3. Processes/Requirements

3.1. The CCG will ensure that it meets its national requirements in respect of its submission of the annual self-assessment IG Toolkit (IGT).

3.2. Non-confidential information about the CCG and its services will be available to the public through a variety of media.

3.3. The CCG will establish and maintain policies to ensure compliance with the Freedom of Information Act 2000. Please refer to the CCG Freedom of Information Policy.

3.4. The CCG will have clear procedures and arrangements for liaison with the press and broadcasting media. Please refer to the CCG Communications Strategy.

3.5. The CCG will have clear procedures and arrangements for handling requests for information from the public. Please refer to the Confidentiality Policy in accordance with the Data Protection Act 1998.

3.6. The CCG will establish and maintain policies to ensure compliance with the Code of Practice for Records Management. Please refer to the CCG Records Management Policy.

4. Legal Compliance

4.1. The CCG regards all Personal Confidential Data (PCD) as confidential except where national policy on accountability and openness requires otherwise.

4.2. The CCG will establish and maintain policies to ensure compliance with the Data Protection Act, Human Rights Act and the common law confidentiality.

4.3. The CCG will establish and maintain protocols for the controlled and appropriate sharing of information with other agencies, taking account of relevant legislation (e.g. Health and Social Care Act 2012, Crime and Disorder Act 1998 and the Protection of Children Act 1999).

5. Information Security

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

5.2. The CCG will promote effective confidentiality and security practice to its staff through policies, procedures and training. Please refer to the CCG Information Security, Email, Portable Devices and Internet policies.

5.3. The CCG will adhere to NHS England's IG SIRI reporting process and will also establish and maintain incident reporting procedures and will monitor and investigate all reported instances of actual or potential breaches. Please refer to the CCG IG SIRI Policy.

6. Information Quality Assurance

6.1. The CCG Executive Committee will establish and maintain policies and procedures for information quality assurance and the effective management of records. Please see the CCG Records Management Policy.

6.2. The CCG will undertake or commission annual assessments and audits of its information quality and records management arrangements.

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

6.4. Wherever possible, information quality should be assured at the point of collection.

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

7. Commissioning of New Services

7.1. The Senior Information Risk Owner (SIRO), and appropriate staff within the NHS South East CSU (SE CSU), should be consulted during the design phase of any new service, process or information asset so that they can decide if a Privacy Impact Assessment (PIA) is required for a particular project or plan.

7.2. Responsibilities and procedures for the management and operation of all information assets should be defined and agreed by the CCG SIRO and the Information Asset Owner (IAO).

8.3. All staff members who may be responsible for introducing changes to services, processes or information assets must be effectively informed about the requirement to seek approval from SE CSU IG PIA Panel that considers IG compliance issues.

8. Responsibilities

8.1. The CCG has a particular responsibility for ensuring that it meets its corporate and legal responsibilities, and for the adoption of internal and external governance requirements. The CCG Governing Body is also responsible for ensuring that sufficient resources are provided to support the requirements of the policy.

8.2. **The CCG Accountable Officer** has overall responsibility for governance in the CCG. As Accountable Officer he/she is responsible for the management of the organisation and for ensuring appropriate mechanisms are in place to support service delivery and continuity.

8.3. **The CCG Caldicott Guardian** is seen as the 'conscience' of the organisation regarding the use of personal confidential data. They are responsible for ensuring all personal confidential data is shared in an appropriate and secure manner.

8.4. **The CCG SIRO** is responsible for leading on Information Risk and for overseeing the development of an Information Risk Policy. For ensuring the Corporate Risk Management process includes all aspects of Information risk. And for ensuring the CCG Governing Body is adequately briefed on information risk issues.

8.5. **The CCG Governing Body Secretary** is responsible for ensuring that this policy is implemented and that IG systems and processes are developed. The role also ensures training is available and is also responsible for the overall development and maintenance of information management practices throughout the CCG.

8.6. **NHS South CSU Associate Director for IT** is responsible, at time of writing, for all aspects of IG relating to IT systems including the production of all relevant IT policies and for the monitoring and audit of the CCG's hosted IT provider. This process is imminently due to be transferred to SE CSU.

8.7. **The CCG Data Custodians'** role is to raise the profile of IG throughout the CCG and to provide local 'champions'. These individuals are directly accountable to the SIRO and will provide assurance that information risk is being managed effectively for their assigned information assets and for

ensuring all staff complete the appropriate modules of the IG Training Toolkit. This role is in addition to their duties and should be fully supported by their manager and recognised in their job description. Data Custodians will also, on an annual basis, be responsible for local assessment of data collections to establish an Information Assets Register (IAR) and Data Flow Mapping (DFM). This important task provides a CCG wide inventory to inform the annual registration with the Information Commissioner's Office (ICO) and highlights potential risk areas that may need risk management intervention. The Data Custodians will be briefed on IG developments and receive specific training.

8.8. Support in the role is available at any time from the SE CSU IG Team. The CCG values staff comments regarding Information handling arrangements and training and it is hoped that each Data Custodian will act as a further conduit to voice these comments.

8.9. NHS South East IG Team defines the CCG policy in respect of IG, taking into account legal and NHS requirements.

8.10. CCG Service Leads are responsible for ensuring that the policy and its supporting standards and guidelines are built into local processes and that there is on-going compliance. Part of this obligation is to ensure that all staff are trained and made aware of confidentiality requirements and procedures. An annual staff questionnaire is undertaken to establish if the current procedures are adequate and effective.

8.11. CCG staff, whether permanent, temporary, contracted, or contractors are responsible for ensuring that they are aware of the requirements of this policy and for ensuring that they comply with these on a day to day basis.

10. Training

10.1. The CCG are required to comply with the CCG Staff IG Handbook which stresses the importance of appropriate information handling which incorporates statutory, common law and best practice requirements. As IG is a framework drawing these requirements together, it is important that staff receive the appropriate training.

10.2. The NHS Operating Framework 'Informatics Planning' requires that the CCG ensures all staff receives annual basic Information Governance training appropriate to their role through the online NHS Information Governance Training Tool. Managers are responsible for monitoring staff compliance.

10.3. On joining the organisation, CCG staff should receive a copy of the Staff IG Handbook.

10.4. All staff are required to undertake IG Training annually. The IG Training Tool should be used wherever possible.

11. Success Criteria

11.1. The CCG IG action plan, along with regular progress reports will be monitored by, Executive Committee.

11.2. Compliance with the IG Toolkit will be assessed by the Health and Social Care Information Centre (HSCIC) including a review of evidence, as part of the CCG performance assessment.

11.3. The CCG will ensure that IG is part of its annual cycle of its programme of internal audit. The Audit will generate an action plan to improve IG management which will monitored by the CCG Executive Committee.

11.4. The results of audits will be reported to the CCG Executive Committee.

11.5. Compliance with CCG policies is required as stipulated in staff contracts of employment. If staff members are unable to follow CCG policies or the policy requirements cannot be applied in a specific set of circumstances, this must be immediately reported to the Line Manager, who should take appropriate action.

11.6. Any non-compliance with CCG policies or failure to report non-compliance may be treated as a disciplinary offence

12. Reference Documentation

- Data Protection Act 1998
- Human Rights Act 1998
- Health and Social Care Act 2012
- Protection of Children Act 1999
- CCG Freedom of Information Policy
- CCG Confidentiality and Data Protection Policy
- CCG Information Security Policy
- HITS IT Security Policy
- CCG Email Policy
- CCG Remote Working and Portable Devices Policy
- CCG Internet Policy
- CCG Risk Management Policy
- CCG Subject Access Request Guidance - Release of Personal confidential data.

13. Consultation and Trials

13.1. In the process of reviewing this document the following personnel have been consulted:

- The CCG Caldicott Guardian
- The CCG Senior Information Risk Owner
- The CCG Governing Body Secretary
- The SE CSU Principle Associate – Information Governance SME
- The SE CSU Senior Associate – Information Governance Compliance

14. Communication and dissemination

14.1. This policy will be communicated and disseminated by electronically by the CCG.

15. Monitoring and Audit

15.1 This policy will be monitored by the Executive Committee to ensure any legislative changes that occur before the review date are incorporated. This policy will also be reviewed biennially, or as appropriate.