Policies for:
Information Governance
Information Quality
Information Management
Information Security

Approved by:	None this version
Date approved:	
Name of originator/author:	Ade Oduntan, Mike Hellier, Graham Hewett
Name of responsible committee/individual:	The Senior Information Risk Owner Information Governance Steering Group
Effective from:	1st April 2014
Review date:	April 2017
Target audience:	NHS Lewisham CCG Employees

Version Control

Version:	0.1
Supersedes:	NHS Lewisham CCG Information Governance Policy (June 2013) NHS Lewisham CCG Information Security Policy and Strategy (June 2013)

Consultation History-

1. **IGSG.**

Implementation

Implementation plan in place?	Yes
Tools for dissemination	Intranet, staff bulletin, mandatory IG training
Date of dissemination	Following Governing Body approval

Scrutiny

Monitoring method	Annual monitoring against the Information Governance Toolkit Standards Review of mandatory training records Review of information governance incidents Internal audit arrangements Information Governance Risk Register
Frequency	Monthly / annually
Responsibility	The Senior Information Risk Owner
Reporting	Information Governance Steering Group and Delivery Committee. Annual Governance Statement and Annual Report

Related Documents

Supporting information, detailed technical guidance and procedures are set out in the NHS Lewisham CCG Information Governance Framework.

Public Sector Equality Duty

The general equality duty requires public sector bodies, in the exercise of their functions, to have due regard to the need to:

- Eliminate discrimination, harassment and victimisation and any other conduct that is prohibited under the Equality Act 2010
- Advance equality of opportunity between people who share a relevant protected characteristic and people who do not share it
- Foster good relations between people who share a relevant protected characteristic and those who do not share it

The NHS Lewisham CCG policies for information governance, information management, information security and information quality ensure that information held about individuals is managed without discrimination or prejudice. The policy sets out how this will be monitored.

Policy Statements

Information Governance

1. NHS Lewisham CCG (the CCG) will be accountable for giving effect to and demonstrating that all the data and information it collects, holds and processes in accordance with the law and best practice, including:
    - The Guide to Confidentiality in Health and Social Care (2013)
    - The Health and Social Care Act (2012)
    - The NHS Constitution
    - The Data Protection Act (1998)
    - The Human Rights Act (1998)
    - Common law duty of confidentiality
    - The Freedom of Information Act (2000)
    - Access to Health Records Act (1990)
    - The Computer Misuse Act (1990)
    - The Fraud Act (2006)
    - The NHS Act (2006)
    - The NHS Code of Practice on Confidentiality (2003)
    - Records Management: NHS Code of Practice (2006)
    - Information Security Management: NHS Code of Practice (2007)
    - The NHS Care Records Guarantee (2011)

2. The CCG will state in its contracts with all organisations from which it commissions services that they must manage information and process data to these same legal requirements and best practice guidance.
3. The CCG will implement a risk (vs. benefits) based approach in its considerations and decisions regarding the privacy and utility of data and information.

Information Quality

4. The CCG will take all reasonable steps to ensure that the information it collects and uses is accurate and complete
5. The CCG will implement appropriate validation checks to support the collection of accurate and complete information and to identify possible errors

Information Management

6. The CCG will proactively use information within the organisation, and with its commissioned and partner organisations both for commissioning the care of service users and for health service management as determined by law, statute and best practice.
7. The CCG will only use information for the purposes that support and are compatible with the delivery of its statutory functions and powers and never for an individual employee's personal gain or purpose.
8. Information when created will be authentic, accurate, accessible, complete, and secure and its integrity will be protected over time.

9. The CCG will put in place measures to ensure that the principles of data minimisation are reflected in its collection and processing of information
10. The CCG will conduct appropriate forms of privacy impact assessment, where relevant.
11. The CCG will put in place measures to ensure that privacy is designed into the processes and controls of its new and changing business endeavours and information systems
12. The CCG will put in place measures to implement and maintain a process to enable individuals (patients and staff) to make complaints and / or challenge the processing being carried out by the CCG.
13. The CCG will make non-confidential information widely available in line with its responsibilities under the Freedom of Information Act 2000.

Information Security

14. The CCG will at all times maintain the confidentiality of information and will confine access to those with appropriate authority and a legitimate reason for access
15. The CCG will take all reasonable and practical steps to reduce the risk of a security breach, data loss or breach of confidentiality
16. The CCG will maintain effective risk management systems to control risks to information security and business continuity
17. The CCG will protect information assets from internal and external threats

Operational and technical guidance and procedures to support these policies are set out in the NHS Lewisham CCG Information Governance Framework.

Scope

18. These policies apply to all the information and data that the CCG collects and processes including personal confidential data (PCD), anonymised or pseudo anonymised data used for commissioning purposes and all corporate records
19. These policies apply to all CCG employees, Governing Body members and all other individuals carrying out the business of the CCG

Responsibilities

Chief Officer

20. The Chief Officer has overall responsibility for ensuring the CCG has appropriate policies and procedures in place to meet its statutory functions for information governance
21. The Chief Officer is responsible for appointing a Senior Information Risk Owner (SIRO) and Caldicott Guardian

Senior Information Risk Owner

22. The SIRO is responsible for the appropriate management of risks associated with the CCG's collection, use and holding of information

23. The SIRO is responsible for ensuring that the CCG makes an appropriate annual submission to the NHS Information Governance Toolkit
24. The SIRO is responsible for leading and fostering a culture that values, protects and uses information for the success of the CCG and benefit of its community
    - Owning the organisation's overall information risk policy and risk assessment processes and ensuring they are implemented consistently by IAOs
    - Advising the Chief Officer or relevant accounting officer on the information risk aspects of his statement on internal controls
    - Owning the CCG's information incident management framework.

Caldicott Guardian

25. The Caldicott Guardian is responsible for leading and advising an assurance framework for the use of PCD within the CCG.
26. The Caldicott Guardian is responsible for giving advice regarding the handling of PCD where there is complexity, overlap and a lack of clarity between direct or indirect care. Her advice should be based on a case by case impact assessment using a benefit versus risk appraisal.

CCG Senior Managers

27. Senior managers are responsible for understanding their roles as "Information Risk Owners" and "Information Asset Owners"
28. Senior managers are responsible for identifying and managing information risks in their remit

CCG Employees

29. All CCG employees are responsible for ensuring that they understand and implement these policies in their day to day work
30. All CCG employees are responsible for ensuring that they complete mandatory information governance training appropriate to their role
31. Employees nominated as "Information Risk Owners" or "Information Asset Owners" and those responsible for operating "information assets" as "Information Risk Administrators" or "Information Asset Administrators" are responsible for the appropriate identification and management of information governance risks

CCG Members

32. GP partners and employees of CCG member practices are required to work to this policy when undertaking roles or work for the CCG

Monitoring Compliance

33. Compliance with these policies will be assessed annually by submission of the Information Governance Toolkit
34. The SIRO will include a statement of compliance with information governance standards in the Annual Governance Statement
35. .In year compliance will be monitored by the Information Governance Steering Group which will report monthly to the Delivery Committee
36. Information Risk Owners will routinely review the risks and information flows associated with the information assets they use to fulfil their role

37. Identified risks to compliance with these policies and the supporting Information Governance Framework will be recorded in the information governance risk register and mitigated in accordance with the CCG's risk management policies and procedures
38. The information governance risk register will be reviewed every month at the Information Governance Steering Group.

Non-Compliance

39. Failure to comply with the requirements of these policies and the supporting Information Governance Framework may result in disciplinary action
40. All information governance incidents should be reported to the CCG's Governance Officer who will record and manage the incidents in accordance with the CCG's incident management procedures
41. the CCG will adopt and utilise the HSCIC Checklist Guidance for Reporting, Managing and Investigating Information Governance Serious Incidents Requiring Investigation
42. Information governance incidents involving PCD should also be reported to the Caldicott Guardian

Training

43. All CCG employees, Governing Body members and all other individuals carrying out the CCG's business must complete annual mandatory information governance training appropriate to their role
44. The SIRO must complete training appropriate to the role
45. The Caldicott Guardian must complete training appropriate to the role

Definitions

Term	Definition	Source
Data	Data is used to describe 'qualitative or quantitative statements or numbers that are assumed to be factual, and not the product of analysis or interpretation.'	Definition taken from The Information Governance Review, Mar 2013 (Gateway Ref: 2900774) based on the Cabinet Office definition
Information	Information is the 'output of some process that summarises interprets or otherwise represents data to convey meaning.'	Definition taken from The Information Governance Review, Mar 2013 (Gateway Ref: 2900774)
Personal Confidential Data or PCD	This term describes personal information about identified or identifiable individuals, which should be kept private or secret. For the purposes of these policies 'personal' includes the Data Protection Act definition of personal data, but it is adapted to include dead as well as living people and 'confidential' includes both information 'given in confidence' and 'that which is owed a duty of confidence' and is adapted to include 'sensitive' as defined in the Data Protection Act.	Definition taken from The Information Governance Review, Mar 2013 (Gateway Ref: 2900774)
Information security	Preservation of confidentiality, integrity and availability of information; in addition, other properties such as authenticity, accountability, non-repudiation and reliability can also be involved	[ISO/IEC 17799:2005]

Further information, technical guidance and procedures to support these polices are set out in the NHS Lewisham CCG Information Governance Framework