NHS
West Hampshire
Clinical Commissioning Group

INFORMATION GOVERNANCE POLICY

Version 3.5

Subject and version number of document:	Information Governance Policy Version 3.5
Serial number:	COR/008/V3.05
Operative date:	1 December 2017
Author:	NHS South, Central & West Commissioning Support Unit
CCG owner:	Mike Fulford, Chief Finance Officer
Links to other (CCG) policies	Freedom of Information Policy Confidentiality & Data Protection Policy Records Management Policy Communications Strategy Information Security Policy Remote Working & Portable Devices Policy Corporate Risk Management Policy
Review date:	April 2018
For action by:	All staff
Policy statement:	To provide a clear information governance framework which includes advice and guidance and to inform staff of their operational and legal responsibilities.
Responsibility for dissemination to new staff:	Line Managers
Mechanisms for dissemination:	This policy will be promoted through the staff briefing and published on the CCG website.
Training implications:	All staff at induction and annual information governance training
Resource implications:	There are no resource implications in relation to this policy.
Further details and additional copies available from:	Website: https://www.westhampshireccg.nhs.uk/documents?media_folder=193&root_folder=Information%20governance%20(IG)%20and%20security
Equality analysis completed?	Yes. Reviewed 29 December 2014 and October 2015. Positive impact on staff and patients protected by the Equality Act 2010 if CCG staff, data custodians / information asset administrators and CSU IG team work in line with this policy. Risk of negative impact if policy breached. Note particular requirements of Section 22 of the Gender Recognition Act 2004 (see Section 4 of this policy, and Appendix 2 of CCG Confidentiality Policy)

Consultation process:	Version 1:WHCCG Corporate Governance Committee – 20 July 2012, approved by Board 2 August 2012 Version 2: WHCCG Corporate Governance Committee – 22 October 2013 Version 3: Nick Birtley, Equality Lead – 29 December 2014 & circulated to members of the CCG Information Governance Group (WHIG) for comment Version 3.02: Policy Sub Group, November 2015 Version 3.5: Policy Sub Group, November 2017
Approved by:	CCG Board
Date approved:	30 November 2017

Website Upload:

Website	Location in FOI Publication Scheme	https://www.westhampshireccg.nhs.uk/documents?media_folder=193&root_folder=Information%20governance%20(IG)%20and%20security
Keywords:	*Insert helpful keywords (metadata) that will be used to search for this document on the intranet and website*	

Amendments Summary:

Amend No	Issued	Page(s)	Subject	Action Date
1	Dec 14	12	9. Amendment to training and re-formatting in line with CCG style guide	
2	Dec 14	5	8.2 Amendment to title -Chief officer replaces accountable officer	
3	Dec 14	9	4.4 Insertion of gender recognition information	
3.02	Oct 15	Throughout	Amendments throughout to bring in line with current terminology.	
3.03	Aug 16	Throughout and page 5	References to Corporate Governance Committee amended to Finance & Assurance Committee throughout and addition of a summary page	17 Aug 16
3.04	Oct 16	Throughout	References to HSCIC and add additional guidance	3 Oct 16
3.05	Oct 17	Throughout	Update to training, inclusion of GDPR statement and update to reference Audit Committee are now responsible for IG.	30 Oct 17

Review Log:

Include details of when the document was last reviewed:

Version Number	Review Date	Name of Reviewer	Ratification Process	Notes
2.0	September 2013	NHS South Commissioning Support Unit Information Governance Team	CCG Corporate Governance Committee: October 2013	Complete review
3.0	December 2014	NHS South CSU IG Team	Corporate Governance Committee	Review
3.02	October 2015	NHS South, Central and West IG Team	CCG Board	Review
3.04	October 2016	NHS South, Central and West IG Team	Policy Sub Group, then CCG Board	Review
3.05	October 2017	NHS South, Central and West IG Team	Policy Sub Group then CCG Board	Review

INFORMATION GOVERNANCE POLICY

Summary of Key Points to Note

This policy provides a clear information governance framework which includes advice and guidance and to inform staff of their operational and legal responsibilities. Specifically:

- To maximise the value of organisational assets by ensuring that information is:
  - Held securely and confidentially
  - Obtained fairly and efficiently
  - Recorded accurately and reliably
  - Used effectively and ethically
  - Shared appropriately and lawfully
- All 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.
- On joining the organisation, CCG staff will receive a copy of the information governance staff handbook and will be required to sign and return a receipt to the CSU IG Team
- All staff are required to undertake information governance training annually. This should be completed through the Information Governance Training Tool or approved face-to-face information governance training delivered by the information governance team.
- 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.
- The senior information risk owner (SIRO), South, Central and West Commissioning Support Unit (CSU) associate director of IT and the CSU head of information governance 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 is required for a particular project or plan.
- 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 CSU IG Privacy Impact Assessment Panel that considers information governance compliance issues.
- All CCG information governance policies and documentation will be reviewed to incorporate information relating to General Data Protection Regulations (GDPR) in readiness for implementation in May 2018.

INFORMATION GOVERNANCE POLICY

CONTENTS

INFORMATION GOVERNANCE POLICY

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 looks at the way the NHS handles information about patients, staff, contractors and the healthcare provided, with particular consideration of personal data and sensitive personal data. 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:

- Held securely and confidentially
- Obtained fairly and efficiently
- Recorded accurately and reliably
- Used effectively and ethically
- Shared appropriately and lawfully

1.5 To protect the organisation’s information assets from all threats, whether internal or external, deliberate or accidental. The CCG will ensure:

- Information will be protected against unauthorised access
- Confidentiality of information will be assured
- Integrity of information will be maintained
- Information will be supported by the highest quality data
- Regulatory and legislative requirements will be met

- Business continuity plans will be produced, maintained and tested
- Information security training will be available to all staff
- All breaches of information security, actual and suspected, will be reported to and investigated by the South, Central & West Commissioning Support Unit (SCW CSU) Information Governance Team

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 confidential data 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 four 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 information governance toolkit.

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. 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 Data Subject Access Request 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 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 duty of 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 (for example, Health and Social Care Act, Health and Social Care (Safety and Quality) Act, Crime and Disorder Act, Protection of Children Act, Section 22 of the Gender Recognition Act 2004)

4.4 Managing protected information about transsexual people. Section 22 of the Gender Recognition Act 2004 says that:

'It is an offence for a person who has acquired protected information in an official capacity to disclose the information to any other person.'

4.5 'Protected information' means information which relates to a person who has made an application under the Gender Recognition Act. This covers both the fact of the application itself and, if the application was successful, the fact that the individual was previously of the opposite gender to the one in which they are now legally recognised. See Confidentiality Policy Appendix 1 for more information.

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, and remote working and portable devices policies.

5.3 The CCG will adhere to NHS Digital's (previously Health and Social Care Information Centre - HSCIC) serious incident requiring investigation (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 information governance handbook document.

6. INFORMATION QUALITY ASSURANCE

6.1 The CCG Finance & Assurance 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), associate director of IT and the head of information governance 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 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 appropriate information asset owner.

7.3 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 NHS South, Central and West Commissioning Support Unit IG Privacy Impact Assessment Panel that considers information governance 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 Finance & Assurance Committee is also responsible for ensuring that sufficient resources are provided to support the requirements of the policy.

8.2 CCG Chief Officer

8.2.1 The CCG chief officer has overall responsibility for governance in the CCG. As chief 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 CCG Caldicott Guardian

8.3.1 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 CCG Senior Information Risk Owner

8.4.1 The CCG senior information risk owner (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 Finance & Assurance Committee is adequately briefed on information risk issues.

8.5 NHS South, Central and West Commissioning Support Unit Head of Information Governance

8.5.1 The head of information governance is responsible for ensuring that this policy is implemented and that information governance systems and processes are developed and training is available and is also responsible for the overall development and maintenance of information management practices throughout the CCG.

8.6 NHS South, Central and West Commissioning Support Unit Information Security Manager

8.6.1 The SCW CSU information security manager is responsible for all aspects of information governance 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.

8.7 CCG Data Custodians / Information Asset Administrators (IAAs)

8.7.1 To raise the profile of information governance throughout the CCG and to provide local ‘champions’, the CCG has established a network of data custodians / IAAs. These individuals are directly accountable to the information asset owner and indirectly 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 information governance training toolkit. This role is in addition to their duties and should be fully supported by their manager and recognised in their job description.

8.7.2 Data custodians / IAAs will also, on an annual basis, be responsible for local assessment of data collections to establish an information assets register (IAR) and also audit staff compliance with Information handling requirements. This important task provides a CCG wide inventory to inform the annual registration with the Information Commissioner and highlights potential risk areas that may need risk management intervention. Information assets (IAs) should include any operating systems, infrastructure, business applications, off the shelf products, services, user-developed applications, records and information held.

8.7.3 The data custodians will be briefed on information governance developments and receive specific training.

8.7.4 Support in the role is available at any time from the CSU information governance team. The CCG values staff comments regarding information handling arrangements and training and it is hoped that each data custodian / IAA will act as a further conduit to voice these comments.

8.8 CCG Board

8.8.1 It is the role of the CCG Board to define the CCG policy in respect of information governance, taking into account legal and NHS requirements.

8.8.2 The CCG Board is also responsible for ensuring that sufficient resources are provided to support the requirements of the policy.

8.9 CCG Audit Committee

8.9.1 The CCG Audit Committee is responsible for overseeing day to day information governance issues; developing and maintaining policies, standards, procedures and guidance, coordinating information governance in the CCG and raising awareness of information governance.

8.10 CCG Service Leads

8.10.1 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. Appendix 1 is a questionnaire to establish if the current procedures are adequate and effective. Data custodians / IAAs are responsible for carrying out annual audits and to implement local remedial actions in response to audit findings.

8.11 **CCG Staff**

8.11.1 All 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.

9. TRAINING

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

9.2 The NHS Operating Framework 'Informatics Planning' and the IG Tookit training requirement requires that the CCG ensures all staff receive~~s~~ annual basic information governance training appropriate to their role. For V12 of the toolkit there was a change to the training requirement which facilitated the option of completing either online training or attending face to face training and completing a short questionnaire - managers are responsible for monitoring staff compliance. However, new staff must complete their first training session online.

9.3 On joining the organisation, CCG staff will receive a copy of the information governance staff handbook and will be required to sign and return a receipt to the CSU IG Team.

9.4 All staff are required to undertake information governance training annually. This should be completed through the E Learning for Health training platform: https://www.e-lfh.org.uk/ or approved face-to-face information governance training delivered by the information governance team.

9.5 Any training undertaken will also be carried out in conjunction with the learning and development team.

10. SUCCESS CRITERIA

10.1 The CCG IG action plan, along with regular progress reports will be monitored by the Audit Committee.

10.2 Compliance with the information governance toolkit will be assessed by NHS Digital including a review of evidence, as part of the CCG performance assessment.

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

10.4 The results of audits will be reported to CCG Audit Committee.

10.5 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.

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

11. REFERENCE DOCUMENTATION

- Data Protection Act 1998
- Human Rights Act 1998
- Health and Social Care Act 2012
- Health and Social Care (Safety and Quality) Act 2015
- Protection of Children Act 1999
- Section 22 of the Gender Recognition Act 2004
- CCG Freedom of Information Policy
- CCG Confidentiality and Data Protection Policy
- CSU ICT Information Security Policy
- CSU ICT Security Incident Handling Policy
- CSU ICT Remote Working and Portable Devices Policy
- CCG Corporate Risk Management Policy
- CCG Subject Access Request Policy

Other

- Care Quality Commission Code of Practice on Confidential Personal Information
- Guide to Confidentiality in Health and Social Care
- NHS England Confidentiality Policy

12. EQUALITY, DIVERSITY AND MENTAL CAPACITY

12.1 This policy was assessed against the South CSU equality impact assessment tool to ensure that it does not introduce any unexpected or unwarranted equality and diversity disparities. The assessment (Appendix 3) confirmed that no amendments are required at this time.

12.2 This policy has been assessed and meets the requirements of the Mental Capacity Act 2005.

12.3 The CCG collects and analyses equalities information (age group, gender, ethnicity, disability status, religion or belief and sexual orientation) about staff and patients in order to comply with the specific duties of the public sector equality duty. This information is anonymised before use and where less than five individuals the information is redacted to prevent potential identification of any individual.

13. MONITORING AND AUDIT

13.1 This policy will be monitored by the Audit Committee to ensure any legislative changes that occur before the review date are incorporated. This policy will also be reviewed annually.

Appendix 1 Confidentiality awareness questionnaire

Confidentiality Awareness Questionnaire

Introduction:

NHS West Hampshire Clinical Commissioning Group (CCG) has a legal obligation to ensure that it manages and safeguards confidential data and have procedures in place to highlight problems such as incidents, complaints or breaches.

Part of this obligation is to ensure that all staff are trained and made aware of confidentiality requirements and procedures. As a result the information governance team would like to ask staff to complete this quick questionnaire so it can establish if the current procedures in place are adequate and effective enough to raise awareness and maintain compliance with confidentiality requirements.

Please return to the IG Team 2nd floor, Omega House, 112 Southampton Road, Eastleigh SO50 5PB when completed for your department.

1) Please state the department you work for: ____________________________

2) Have you received any of the following training regarding confidentiality whilst working at the CCG;

a. Induction Training? ____

b. Information Security and Confidentiality training / Information Governance Training? ____

3) Can you provide an approximate date of your most recent confidentiality based training or information received? (**this may be a leaflet or poster**)

____

4) If you have any concerns or issues regarding confidentiality to whom would you turn to for advice?

____

5) What would you do if you suspect a possible breach of confidentiality?

____

____

6) If a patient's or staff's record goes missing, are you aware of the procedures / policy to follow (please specify if known)?

____

____

7) Can you name any of the policies that the CCG follows on confidentiality?

____

____

____

8) Where would you find them?______________________________________

9) Name one of the main acts of parliament that has confidentiality as its central focus? ____

10) Who is your department's data custodian / IAA? ________________________

____

11) Who is you department's information asset owner? ____________________

____

12) Can you name your Caldicott Guardian? ______________________________

____

13) Can you name your senior information risk owner? ____________________

____

14) If a patient or staff requests a copy of the information you hold:

Who would you inform? ____

Do you have to release the records? ________________________________

How long do you have to respond? __________________________________

15) Any other comments in reference to confidentiality you may have:

____

____

Appendix 2 Analysing the impact on equality

1.	**Title of policy/ programme/ framework being analysed** Information Governance Policy
2.	**Please state the aims and objectives of this work and the *intended equality outcomes*. How is this proposal linked to the organisation's business plan and strategic equality objectives?** To provide NHS West Hampshire Clinical Commissioning Group (CCG) staff with a clear information governance framework which includes advice and guidance and to inform staff of their operational and legal responsibilities.
3.	**Who is likely to be affected? e.g. staff, patients, service users, carers** Staff, patients and carers
4.	**What evidence do you have of the potential impact (positive and negative)?** If CCG staff, data custodians and the CSU IG Team handle information about staff and patients in line with this and related policies there will be a positive impact for people protected by the Equality Act 2010. Breaches of this policy could have a negative impact. The CCG collects and analyses equality information about staff and patients to enable it to comply with the specific duties of the public sector equality duty. This information is anonymised before use and where the number of individuals is less than 5, the data is redacted to avoid potential identification of individuals.
4.1	**Disability** (Consider attitudinal, physical and social barriers) Positive impact if this and related policies are followed.
4.2	**Sex** (Impact on men and women, potential link to carers below) Positive impact if this and related policies are followed.
4.3	**Race** (Consider different ethnic groups, nationalities, Roma Gypsies, Irish Travellers, language barriers, cultural differences). Positive impact if this and related policies are followed
4.4	**Age** (Consider across age ranges, on old and younger people. This can include safeguarding, consent and child welfare). Positive impact if this and related policies are followed
4.5	**Gender reassignment** (Consider impact on transgender and transsexual people. This can include issues such as privacy of data and harassment). Positive impact if this and related policies are followed. Note particular requirements under Section 22 of the Gender Recognition act 2004 outlined in Section 4 of this policy and Confidentiality Policy Appendix 1.

4.6 Sexual orientation (This will include lesbian, gay and bi-sexual people as well as heterosexual people).

Positive impact if this and related policies are followed

4.7 Religion or belief (Consider impact on people with different religions, beliefs or no belief)

Positive impact if this and related policies are followed

4.8 Marriage and Civil Partnership

Positive impact if this and related policies are followed

4.9 Pregnancy and maternity (This can include impact on working arrangements, part-time working, infant caring responsibilities).

Positive impact if this and related policies are followed

4.10 Carers (This can include impact on part-time working, shift-patterns, general caring responsibilities, access to health services, 'by association' protection under equality legislation)**.**

Positive impact if this and related policies are followed

4.11 Additional significant evidence

Give details of any evidence on other groups experiencing disadvantage and barriers to access due to:

- socio-economic status
- location (e.g. living in areas of multiple deprivation)
- resident status (migrants)
- multiple discrimination
- homelessness

Positive impact if this and related policies are followed

5 Action planning for improvement

Please give an outline of the key action points based on any gaps, challenges and opportunities you have identified. An Action Plan template is appended for specific action planning.

None identified

Name of person who carried out this analysis

Nick Birtley, Equality and Diversity Lead, West Hampshire CCG
Lucy, Information Governance Manager, South, Central and West Commissioning Support Unit

Date analysis completed

3 October 2013
Reviewed 29 December 2014
Reviewed October 2015