North East Hampshire and Farnham
Clinical Commissioning Group

INFORMATION GOVERNANCE FRAMEWORK

Subject and version number of document:	INFORMATION GOVERNANCE FRAMEWORK
Serial Number:	IG Policy
Operative date:	7th September 2016
Author:	IG Team, NHS South, Central and West Commissioning Support Unit Jackie Thomas, Information Governance Manager, South, Central and West CSU
Review date:	August 2017
For attention of:	All NHS North East Hampshire & Farnham Clinical Commissioning Group staff. Information Governance Team.
Policy statement:	This Information Governance Framework Policy aims to capture the NHS North East Hampshire and Farnham Clinical Commissioning Group's (CCG) approach to information governance.
Responsibility for dissemination to new staff:	NSH North East Hampshire and Farnham Clinical Commissioning Group Managers
Training Implications:	No specific training required
Further details and additional copies available from:	NEHF CCG Governance Team
Equality Impact Assessment Completed?	The content of this policy does not raise any equality and diversity issues in relation to the protected characteristics
Approved by:	North East Hampshire & Farnham CCG Audit & Risk Committee
Date approved:	7th September 2016

Intranet and Website Upload:

Intranet	Electronic Document Library Location:	To be confirmed
Website	Location in FOI Publication Scheme	To be confirmed
Keywords:	Information Governance Framework	

Amendments Summary:

Amend No	Issued	Page(s)	Subject	Action Date
1.V3		(page 4)	Inclusion of IG SIRI Incident Management and Reporting Procedure, Guidance document for new process (PIA's) and Codes of Practice	November 2014
2.V3		Item 1, page 4	Inclusion of Health & Social Care Act 2012 and Health & Social Care Act 2015.	November 2015
3.V3		Item 3, page 9	Update to current version of NHS Operating Framework	November 2015
4.V3		App 1, page 13	Equality Impact Assessment reviewed	November 2015
5.V3		Throughout document	Update to reflect CSU organisation name change to South, Central & West CSU	November 2015
1.V4		Item 1, page 5 Item 4.1, page 10 Appendix 1, page 13	Annual review in line with CCG and IG Toolkit requirements. Updated with minor amendments to include reference to Code of Practices on confidential information, HSCIC name change to NHS Digital and reviewed Equality Impact Assessment	August 2016

Review Log:

Include details of when the document was last reviewed:

Version Number	Review Date	Name of Reviewer	Ratification Process	Notes
1.0	January 2014	NHS South CSU, Information Governance Team		
2.0	November 2014	Jackie Thomas, Information Governance Manager South CSU		
3.0	November 2015	Jackie Thomas, Information Governance Manager South, Central and West CSU		
4.0	August 2016	Jackie Thomas, Information Governance Manager South, Central and West CSU		10/11/16 Inclusion of IT Assurance Plan and IT Framework date of approval

1. Introduction

This Information Governance Framework document aims to capture the NHS North East Hampshire & Farnham Clinical Commissioning Group's (CCG) approach to information governance.

Robust Information Governance (IG) requires clear and effective management and accountability structures, governance processes, documented policies and procedures, trained staff and adequate resources. The way that an organisation chooses to deliver against these requirements is referred to within the Information Governance Toolkit as the organisation's Information Governance Management Framework. This Framework will be approved by the Audit & Risk Committee and reviewed annually.

This Information Governance Framework must be read in conjunction with the CCG Information Governance Policy.

There are many different standards and legislation that apply to information governance and information handling, including:

- Data Protection Act 1998
- Access to Health Records Act 1990
- Freedom of Information Act 2000
- Caldicott Guidance
- Human Rights Act 1998
- Public Records Act 1958
- Records Management NHS Code of Practice
- Mental Capacity Act 2005
- Common Law Duty of Confidentiality
- Confidentiality NHS Code of Practice
- International information security standard: ISO/IEC 27002: 2005
- Information Security NHS Code of Practice
- Current performance standards (NHS Information Governance Toolkit)
- Computer Misuse Act 1990
- Copyright, Designs and Patents Act 1988
- Health and Social Care Act 2012
- Health and Social Care Act (Quality & Safety) 2015

The Framework's policies

A formal information security risk assessment and management programme for key information assets has been documented, implemented and reviewed in compliance with ISO27001. IG requirement 341, 1b mandates that this is included within the IG Framework document – (requirement 130). The IT Security Assurance Plan and IT Security Framework which relate to this were approved on the 10th November 2016 by the Information Governance Steering Group in the Commissioning Support Unit.

The Information Governance Framework should be read in conjunction with other policies:

i) Information Governance
ii) Data Subject Access Request
iii) Information Security
iv) Confidentiality
v) Safe Haven
vi) Records Management

ICT policies can be found on the CCG intranet.

These policies will be reviewed every 3 years unless legislative changes are required prior to this time.

The Framework's Procedures:

Information Governance SIRI Incident Management and Reporting Procedure

Guidance:

Guidance for the Introduction of New Processes (Privacy Impact Assessments)

Codes of Practice:

- **Data Sharing** - Data Protection Code of Practice - ICO
- **NHS Code of Practice: Records Management -** Records management: NHS code of practice: Department of Health - Publications
- **Confidentiality: NHS Code of Practice** - Confidentiality: NHS Code of Practice - Publications - Inside Government - GOV.UK
- **Confidentiality Supplementary Guidance** - Confidentiality: NHS Code of Practice - supplementary guidance: public interest disclosures - Publications - Inside Government - GOV.UK
- **CCTV -** http://www.ico.org.uk/~/media/documents/library/Data_Protection/Detailed_specialist_guides/ICO_CCTVFINAL_2301.pdf
- **Privacy Notices Code of Practice** - Data Protection - ICO
- **Annonymisation -** http://www.ico.org.uk/Global/~/media/documents/library/Data_Protection/Practical_application/anonymisation_code.ashx
- **Personal Information Online Code of Practice** - http://www.ico.org.uk/~/media/documents/library/Data_Protection/Detailed_specialist_guides/personal_information_online_cop.pdf

Other

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

The Caldicott Principles

The CCG fully supports and has adopted the Caldicott principles (2013) and these under pin the framework.

Principle 1 – Justify the purposes (s)

Every proposed use or transfer of personal confidential data within or from an organisation should be clearly defined, scrutinised and documented, with continuing uses regularly reviewed, by an appropriate guardian.

Principle 2 – Don't use personal confidential data unless it is absolutely necessary

Personal confidential data should not be included unless it is essential for the specified purpose(s) of that flow. The need for patients to be identified should be considered at each stage of satisfying the purpose(s).

Principle 3 – Use the minimum necessary personal confidential data

Where use of personal confidential data is considered to be essential, the inclusion of each individual item of data should be considered and justified so that the minimum amount of personal confidential data transferred or accessible as is necessary for a given function to be carried out.

Principle 4 – Access to personal confidential data should be on a strict need to know basis

Only those individuals who need access to personal confidential data should have access to it, and they should only have access to the data items that they need to see. This may mean introducing access controls or splitting data flows where one data flow is used for several purposes.

Principle 5 – Everyone with access to personal confidential data should be aware of their responsibilities

Action should be taken to ensure that those handling personal confidential data – both clinical and non-clinical staff – are made fully aware of their responsibilities and obligations to respect patient confidentiality.

Principle 6 – Comply with the Law

Every use of personal confidential data must be lawful. Someone in each organisation handling personal confidential data should be responsible for ensuring that the organisation complies with legal requirements.

Principle 7 – The duty to share information can be as important as the duty to protect patient confidentiality

Health and social care professionals should have the confidence to share information in the best interests of their patients within the framework set out by these principles. They

should be supported by the policies of their employers, regulators and professional bodies.

The Department of Health has developed standards of information governance requirements and compliance is measured by the Information Governance Toolkit (IGT). The CCG will complete this annual self-assessment tool. The requirements of the IGT cover all aspects of information governance including:

- Information Governance Management
- Confidentiality and Data Protection Assurance
- Information Security Assurance
- Clinical Information Assurance
- Secondary Use Assurance
- Corporate Information Assurance

2. Strategic Aims

The aim of this Framework is to set out how the CCG will effectively manage Information Governance. The organisation will achieve compliance by:

- Establishing robust information governance processes that conform to NHS England and the Health and Social Care Information Centre standards and comply with relevant legislation.
- Establishing, implementing and maintaining policies for the effective management of information.
- Providing clear advice and guidance to staff to ensure that they understand and apply the principles of information governance to their working practice.
- Sustaining an Information Governance culture through increasing awareness and promoting Information Governance, thus minimising the risk of breaches of personal data.
- Assessing CCG performance using the Information Governance Toolkit and Internal Audits and developing and implementing action plans to ensure continued improvement.

3. Roles and Responsibilities

Audit & Risk Committee

The CCG Governing Board has delegated its function for information governance to the Audit & Risk Committee. It is therefore the responsibility of the Audit & Risk Committee to ensure that the organisation corporately meets it legal responsibilities and for the adoption of internal and external governance requirements. Specifically, the Audit & Risk Committee will:–

- support the Governing Body in its governance and oversight role

- provide assurance to the Governing Body that work is undertaken to achieve at least level 2 performance against all requirements identified in the IG Toolkit and production of clear improvement plans to achieve level 2 for all other standards has been completed

The Audit & Risk Committee will be updated on IG issues via quarterly reports produced by the NHS South, Central and West Commissioning Support Unit (CSU) IG Lead which has delegated responsibility for monitoring IG standards within the organisation.

The Chief Finance Officer as the Senior Information Risk Owner (SIRO) will bring to the CCG's attention individual issues relating to IG not covered in the Audit & Risk Committee IG Updates reports.

Clinical Commissioning Group Chief Officer

The Chief Officer has overall responsibility for Information Governance within the CCG. As Accountable Officer, she is responsible for the management of Information Governance and for ensuring appropriate mechanisms are in place to support service delivery and continuity. Information Governance provides a framework to ensure information is used appropriately and is held securely.

Clinical Commissioning Group Senior Information Risk Owner (SIRO)

The Senior Information Risk Owner (SIRO) role is held by the CCG Finance Officer. The SIRO role will identify and manage the information risks to the CCG and with its partners. This includes oversight of the organisation's information security incident reporting and response arrangements and the Registration Authority business process.

Clinical Commissioning Group Caldicott Guardian

The Caldicott Guardian is a senior person responsible for protecting the confidentiality of patient and service-user information and enabling appropriate information sharing.

Acting as the 'conscience' of an organisation, the Caldicott Guardian will actively support work to enable information sharing where it is appropriate to share, and will advise on options for lawful and ethical processing of information. The Caldicott Guardian will also have a strategic role which involves representing and championing Information Governance requirements and issues at executive team level and where appropriate, at a range of levels within the organisation's overall governance framework.

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

The Information Security Manager for the CSU is responsible for the implementation and enforcement of information security within the CCG.

NHS South, Central and West Commissioning Support Unit Information Governance Service Lead

The Head of Information Governance for the CSU has been appointed to act as the overall Information Governance lead for the CCG and under the approved arrangements.

The Head of Information Governance will be responsible for ensuring all tasks are undertaken in order to meet the required standards.

Key tasks will include:-

- Developing and maintaining the currency of comprehensive and appropriate documentation that demonstrates commitment to and ownership of IG responsibilities, e.g. the production of an overarching high level Framework document supported by relevant policies and procedures.
- Ensuring that there is top level awareness and support for IG resourcing and implementation of improvements within the CCG.

- Establishing working groups, if necessary, to co-ordinate the activities of staff given IG responsibilities and progress initiatives;
- Ensuring annual assessments and audits of IG and other related policies are carried out, documented and reported;
- Ensuring that the annual assessment and improvement plans are prepared for approval by the CCG Audit & Risk Committee in a timely manner.
- Ensuring that the approach to information handling is communicated to all staff and made available to the public;
- Ensuring that appropriate training is made available to staff and completed as necessary to support their duties. For NHS organisations this will need to be in line with requirements of the current version of the Informatics Planning component of the NHS Operating Framework;
- Liaising with other committees, working groups and programme boards in order to promote and integrate Information Governance standards;
- Monitoring information handling activities to ensure compliance with law and guidance;
- Providing a focal point for the resolution and/or discussion of Information Governance issues.

All Staff

The majority of staff handle information in one form or another. Staff who in the course of their work create, use or otherwise process information have a duty to keep up to date with, and adhere to, relevant legislation, case law and national guidance.

The CCG's policies and procedures will reflect such guidance and compliance with these polices and will ensure a high standard of IG compliance within the organisation. All staff, whether permanent, temporary, contracted or contractors are responsible for ensuring that they are aware of their responsibilities in respect of IG.

A breach of confidentiality may be treated as a serious disciplinary incident, which in some circumstances may lead to dismissal. All staff should ensure that they are aware of the relevant policies and procedures in respect of any personal information they may process.

Information Asset Owners (IAOs)

Designated Information Asset Owners are senior members of staff who provide assurance to the SIRO that information risks, within their respective areas of responsibility, are identified and recorded and that controls are in place to mitigate those risks.

Data Custodians

Information Asset Owners can appoint Data Custodians to support in the delivery of their information risk management responsibilities. Data Custodians ensure that policies and procedures are followed; recognise actual or potential security incidents and take steps to mitigate those risks, consult with their IAO on incident management and ensure that information asset registers are accurate and up to date.

All staff, whether permanent, temporary, contracted or contractors are responsible for ensuring that they are aware of their responsibilities in respect of Information Governance.

4. Information Governance Management

4.1 Principles

There should be proactive use of information within the organisation, both for service users and service management as determined by law, statute and best practice.

There should also be proactive use of information between the CCG, NHS Trusts and partner organisations to support patient care as determined by law, statute and best practice.

The CCG will establish and maintain policies and procedures to ensure compliance with requirements contained in the NHS Information Governance Toolkit sponsored by NHS Digital (previously Health and Social Care Information Centre, HSCIC).

The CCG will annually assess its performance against the requirements set out in the IG Toolkit and will report the results of its self-assessment on NHS Digital – IG Toolkit in accordance with current guidance.

The CCG will follow a Programme of continual improvement to increase IG compliance year on year.

Where appropriate the principles of information management and handling outlined in this policy are to be applied to identifiable information about the CCG staff as well as service users.

4.2 Openness

The CCG recognises the need for an appropriate balance between openness and confidentiality in the management and use of information.

Information will be defined and where appropriate kept confidential, underpinning the principles of Caldicott and the regulations outlined in the Data Protection and Freedom of Information Acts.

Non-confidential information relating to the CCG and its services will be available to the public through a variety of means including the procedures established to meet requirements under the Freedom of Information Act 2000.

4.3 Training

The CCG recognises the importance of an effective training structure and Programme to deliver compliant awareness of IG and its integration into the day-to-day work and procedures.

All permanent/contract staff will complete the online mandatory training modules within the first four weeks of employment, with further training required for managers, team leaders, and staff who process personal information, and staff with specific information roles.

4.4 Audit and Monitoring compliance with this framework

The CCG will use a variety of methods to monitor compliance with the processes detailed in this document, including as a minimum the following two methods:

IG Toolkit
Overall compliance with this policy will be reviewed annually through the review arrangements required by the IG Toolkit and will be reported to the appropriate committee.

IG Incidents
Information Governance compliance will be monitored through the monitoring of reported IG incidents.

The Audit & Risk Committee will be responsible for providing assurances that the IG organisational framework is adequate for providing clear guidance in the event of significant changes which may affect the policy.

The Audit & Risk Committee will ensure that adequate arrangements exist for:

- Reporting incidents, Caldicott issues
- Analysing and upward reporting of incidents and adverse events
- Reporting IG work programmes and progress reports
- Reporting IGT assessments and improvement plans
- Communicating IG developments

In addition to the monitoring arrangements described above, the CCG may undertake additional monitoring of this framework in response to the identification of any gaps, or as a result of the identification of risks arising from the framework prompted by incident review, external reviews or other sources of information and advice.

4.5 Procedure Review

In line with the organisation's key documents this document will be reviewed annually in line with IG Toolkit requirements unless new, revised legislation or national guidance necessitates an earlier review.

4.6 Dissemination and Implementation

The policy will be publicised on the CCG intranet. Managers will be required to ensure that their staff understand its application to their practice.

Awareness of any new content/change in process will be through the staff bulletin, in the first instance. Where a substantive revision is made then a separate plan for communicating and implementing this change will be devised by the Audit & Risk Committee

4.7 Equality Impact Assessment

The CCG recognises the diversity of the local community and those in its employment. The organisations aim to provide a safe environment free from discrimination and a place where all individuals are treated fairly, with dignity and appropriately to their need.

This policy was assessed against the NHS South, Central and West CSU Impact Assessment tool to ensure that it does not introduce any unexpected or unwarranted equality and diversity disparities. The assessment confirmed that no amendments are required at this time and is outlined in Appendix 1.

Approved by:

Date:

Review Date: August 2017

APPENDIX 1 – EQUALITY IMPACT ASSESSMENT

Analysing the Impact on Equality

1. Title of policy/ programme/ framework being analysed Information Governance Framework
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? This Information Governance Framework document aims to capture the NHS North East Hampshire & Farnham CCG Clinical Commissioning Group's (CCG) approach to information governance.
3. Who is likely to be affected? e.g. staff, patients, service users, carers Staff, patients, service users
4. What evidence do you have of the potential impact (positive and negative)? None expected.
4.1 Disability (Consider attitudinal, physical and social barriers) No impact
4.2 Sex (Impact on men and women, potential link to carers below) No impact
4.3 Race (Consider different ethnic groups, nationalities, Roma Gypsies, Irish Travellers, language barriers, cultural differences). No impact
4.4 Age (Consider across age ranges, on old and younger people. This can include safeguarding, consent and child welfare). No impact
4.5 Gender reassignment (Consider impact on transgender and transsexual people. This can include issues such as privacy of data and harassment). No impact
4.6 Sexual orientation (This will include lesbian, gay and bi-sexual people as well as heterosexual people). No impact
4.7 Religion or belief (Consider impact on people with different religions, beliefs or no belief) No impact
4.8 Marriage and Civil Partnership No impact
4.9 Pregnancy and maternity (This can include impact on working arrangements, part-time

working, infant caring responsibilities).
No impact

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)**.**
No impact

4.11 Additional significant evidence (See Guidance Note)
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

No impact

5 Action planning for improvement (See Guidance Note)
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
Jackie Thomas, Information Governance Manager, South, Central and West CSU

Date analysis completed
25 August 2016