North East Essex
Clinical Commissioning Group

Information Governance Policy

NEECCG POLICY REFERENCE: NEE/CCG/2013/014

Target Audience	Board members, sub-committee members and all staff working for, or on behalf of, the NEE CCG
Brief Description (max 50 words)	This policy outlines the organisation's approach to the management of Information Governance and information handling. It explains the accountability and reporting arrangements for Information Governance and how assurance is provided to meet at least the minimum standards of Information Governance compliance required by the NHS Information Governance Toolkit. *Compliance with all North East Essex CCG policies, procedures, protocols, guidelines, guidance and standards is a condition of employment. Breach of policy may result in disciplinary action.*
Action Required	Once this policy has been approved, it will be disseminated to all staff and placed on the CCG website/staff Intranet,

Document Information

Title /Version Number/(Date)	Information Governance Policy/ Version 3.2/November 2016
Accountable Executive	Chief Finance Officer
Responsible Post holder/Policy Owner	Information Governance Team
Date Approved	7th November 2016
Approved By	Quality Committee
Review Date	March 2019
Equality Impact Assessment	**EQUALITY IMPACT ASSESSMENT** This document has been assessed for equality impact on the protected groups, as set out in the Equality Act 2010. This Policy is applicable to the Board, every member of staff within the CCG irrespective of their age, disability, sex, gender reassignment, pregnancy, maternity, race (which includes colour, nationality and ethnic or national origins), sexual orientation, religion or belief, marriage or civil partnership, and those who work on behalf of the CCG

Brief Summary:
This policy outlines the organisation's approach to the management of Information Governance and information handling. It explains the accountability and reporting arrangements for Information Governance and how assurance is provided to meet at least the minimum standards of Information Governance compliance required by the NHS Information Governance Toolkit.

Document Management

Version	Date Issued	Details	Brief Summary of Change	Author
1.0	15/01/2013	Draft	New document	NHS Essex Commissioning Support Unit, Information Governance Team
1.1	14/02/2013	Final	Approved by North East Essex CCG Board	NHS Essex Commissioning Support Unit, Information Governance Team
2.0	24/10/201	Draft	Changes in guidance and reporting structure necessitates policy review	CCGs Information Governance Team (Hosted by Basildon and Brentwood CCG)
2.1	28/11/2014	Draft	Amended following comments from IG Steering Group	CCGs Information Governance Team (Hosted by Basildon and Brentwood CCG)
2.2	28/01/2015	Draft	Format changes only; content of policy remains unchanged.	North East Essex CCG
2.3	07/04/2015	Final	CCG Board approval on 31st March 2015 reflected within policy. Following Board comments key contacts within CCG on page 12 updated.	North East Essex CCG
3.0	22/08/2016	Draft	Amendments and format changes for current year	CCGs Information Governance Team (Hosted by Basildon and Brentwood CCG)
3.1	26/10/2016	Draft	Personalise and document review	North East Essex CCG
3.2	07/11/2016	Final	Approved by Quality Committee	North East Essex CCG

Contents

1. Introduction

Information is a vital asset, NHS North East Essex Clinical Commissioning Group (the CCG) therefore recognises the importance of reliable information, both in terms of the clinical management of individual patients and the efficient management of services and resources. Information Governance plays a key part in supporting clinical governance, service planning and performance management.

It also provides the necessary assurance to the CCG and to individuals that all personal information is dealt with legally, securely and efficiently, in order to deliver the best possible care to all concerned.

The CCG will establish and maintain policies and procedures to ensure compliance with requirements contained in the National Health Service Department of Health / Health & Social Care Information Centre Information Governance Toolkit. It will do this with management accountability and structures and by providing a robust governance framework for information management.

2. Purpose

The purpose of this policy is to provide guidance for the CCG and all staff members that will facilitate effective management of all information assets and associated resources. This document is directed to all CCG employees, Governing Body members, lay members, trainees, contractors, temporary staff, providers of services that the CCG commissions and anyone who is involved in any processing of information, at any level, within or on behalf of the organisation, or who may be given access to areas in which information is stored within the CCG.

The document will be accessible to staff via the CCG staff intranet and shared drive and it will be available to the public via our publication scheme on the CCG public website. The document will also be brought to the attention of staff via the IG training programme.

3. Scope

This policy covers all aspects of information within the organisation, including but not limited to:

- Patient / / Service User Information
- Staff Information
- Organisational Information
- Structured record systems (including clinical) – paper and electronic
- Transmission of information – fax, e-mail, post and telephone

This policy covers all information systems purchased, developed and managed by / or on behalf of the organisation and any individual directly employed or otherwise by the organisation.

4. Definitions and terms

HSCIC- Health & Social Care Information Centre (now NHS Digital)

IGT- IG Toolkit

PCD- Personal Confidential Data

PID- Person Identifiable Data

NHS Digital- formerly HSCIC

TNA- Training Needs Analysis

5. Roles and Responsibilities

Accountable Officers for NHS North East Essex CCG

The Chief Officer, as the Accountable Officer, has overall responsibility for information governance within the CCG. The Chief Officer is responsible for the management of Information Governance and for ensuring appropriate mechanisms are in place to support service delivery and continuity.

Senior Information Risk Owner (SIRO) for NHS North East Essex CCG

The role of Senior Information Risk Owner (SIRO) in the CCG has been assigned to the Chief Officer. The SIRO takes ownership of the organisation's information risks policy and acts as advocate for information risk on the CCG Governing Body and Quality Committee. This includes oversight of information security incident reporting and response arrangements.

Caldicott Guardian for NHS North East Essex CCG

The Caldicott Guardian has particular responsibilities for protecting the confidentiality of patients / service-user's information and enabling appropriate sharing. For the CCG, this is the Director of Nursing and Clinical Quality. Acting as the 'conscience' of the 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.

Head of IG

The Head of Information Governance / Data Protection Officer (DPO) is responsible for ensuring the CCG complies with all aspects of Information Governance and the Data Protection Act. The

Head of Information Governance will ensure all tasks are undertaken in order to meet the required standards.

Freedom of Information Lead

The Freedom of Information (FOI) Lead's main responsibilities are:

- To ensure the CCG's compliance with all aspects of the Freedom of Information Act, associated Codes of Practice and related provisions in particular for contracting and procurement, minutes of meetings and so on.
- To provide reports to the Quality Committee highlighting resource, performance and compliance issues
- To draft and / or maintain the currency of the organisation's FOI policy
- To ensure training and written procedures are widely disseminated and available to all staff
- To ensure the general public has access to information about their rights under the Act

All Staff

The majority of staff handle information in one form or another. Staff that 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 policies and procedures will reflect such guidance and compliance with these strategies and will ensure a high standard of Information Governance compliance within the organisation. All staff and officers, whether permanent, temporary, contracted, agency or contractors are responsible for ensuring that they are aware of their responsibilities in respect of Information Governance.

All staff who use any level of information must:

- Be aware of and understand their responsibilities
- At all times comply with policies and procedures issued by the CCG
- Work within the principles outlined in the Information Governance Framework
- Complete, on an annual basis, Information Governance training, relevant to their job role
- Always follow best practice, as trained or instructed to do so
- Ensure that information related incidents are reported to line management
- Seek advice or guidance if needed without delay
- Report all information related security incidents and near misses

Information Asset Owners (IAOs)

Designated Information Asset Owners (IAOs) are senior members of staff at director / assistant director level or heads of department responsible for providing 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.

Information Asset Administrators (IAAs)

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

Responsibilities of the CCG

All information used within the NHS is subject to handling by different departments and individuals. At no time should the confidentiality of this information ever be compromised.

Therefore in order to safeguard adequately at all times it is vitally important that all individuals are clear about their responsibilities. In order to ensure clarity amongst all concerned, the CCG will fully promote and support the mandatory completion of appropriate education and training.

The CCG will ensure that all legal requirements are met.

To manage its obligations the CCG will issue and support standards, policies and procedures, ensuring that information is held, obtained, recorded, used and shared correctly.

Patients / service users rights shall be respected, they will receive assurances that their information is handled in accordance with the law. An effective and well advertised procedure will be put into place for all concerned to clearly establish the process by which they can raise any concerns that they may have.

6. Principles

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, clinical and information governance and recognises it's public accountability, but equally places importance on the confidentiality of and, the security arrangements, to safeguard both personal information about patients, staff and that of a commercially sensitive nature.

The CCG also recognises the need to share patient information with other health and social care organisations and agencies legally and in a controlled and consistent manner, with the interests of the patient always at the forefront. The CCG also recognises its responsibilities in line with the Freedom of Information Act 2000, in particular the public interest test.

The CCG believes that accurate, timely and relevant information is fundamentally essential in continuing to deliver the highest quality health care throughout Essex. As such it is the responsibility of all clinical and non-clinical staff to ensure and promote the quality of information and to actively use this effectively in decision making processes.

7. Information Governance Framework

Information will be defined and where appropriate kept confidential, underpinning the Caldicott Principles and the regulations outlined within the Data Protection Act 1998. Non-confidential information of the CCG and associated services will be made available to the public, in line with the requirements of the Freedom of Information Act 2000, via a CCG publication scheme.

Patients will have access to information relating to their own healthcare, options for treatment available and their rights to have choice. There will be clear procedures and arrangements for handling queries from patients and the public for staff to follow.

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

Integrity of information will be developed, monitored and maintained to ensure that it is appropriate and fit for the purposes intended.

Availability of information for operational purposes will be maintained within set parameters relating to its importance via appropriate procedures and computer system resilience.

The CCG regards all identifiable personal information relating to patients as confidential. Compliance with legal and regulatory frameworks will be achieved, monitored and maintained.

The CCG regards all identifiable personal information relating to staff as confidential except where national policy on accountability and openness requires otherwise.

The CCG will establish and maintain policies and procedures to ensure compliance with the Data Protection Act 1998, Human Rights Act (1998), Freedom of Information Act 2000 and the common law duty of confidentiality.

Awareness and understanding of all staff with regard to their responsibilities, will be routinely assessed and appropriate instruction and awareness provided through induction and mandatory training sessions.

Risk assessment, in conjunction with overall priority planning of organisational activity will be undertaken to determine that the appropriate, effective and affordable information governance controls are in place.

Information Governance Management

Information Governance Management across the CCG will be coordinated by the Information Governance Team via the Information Governance Steering Group, which is accountable to the Quality Committee.

The Information Governance Team will be responsible for but not limited to:

- Recommending related policies and procedures for approval to the Quality Committee,
- Recommending the annual submission of compliance with the requirements for the Information Governance Toolkit and related action plan for approval to the Quality Committee
- To co-ordinate and monitor the Information Governance agenda across the CCG

Confidentiality & Data Protection

- The CCG has appointed a Senior Information Risk Owner (SIRO) to lead on the management of all risks
- The CCG has appointed a Caldicott Guardian who will be responsible for establishing good practice across the CCG
- The CCG will establish and maintain policies and procedures to ensure compliance with the Caldicott Principles and the NHS Confidentiality Code of Practice
- The CCG will promote confidentiality through policies, procedures and staff training
- The CCG will support the Caldicott Programme through the Information Governance Steering Group
- The CCG will ensure the Declaration to the Information Commissioner reflects the information needs of the CCG
- The CCG will promote the Data Protection Act 1998 and provide support to staff through policies, procedures and training to ensure compliance

Information Security Assurance

The CCG will establish and maintain policies for the effective and secure management of its information assets and resources. Audits will be undertaken to assess information and IT security arrangements. The CCG's incident reporting system will be used to report, monitor and investigate all breaches of confidentiality and security.

Clinical and Corporate Information Assurance

- The CCG will establish and maintain policies for information quality assurance. Audits will be undertaken by the CCG on quality of data and records management arrangements
- Information Asset Owners (IAOs) and managers will be expected to take ownership of, and seek to improve, the quality of data within business areas under their responsibility
- Wherever possible, information quality will be assured at the point of collection

- The CCG will promote data quality through policies, procedures and user manuals and training
- The CCG will promote effective records management through policies, procedures and training
- The CCG will use "Records Management: NHS Code of Practice, Part 1 and Part 2" as its standard, for the management of all records
- The CCG Governing Body will be issued with copies of all of the above to increase awareness between all and to ensure that full support is received from the Governing Body.

8. Information Sharing

The sharing of Personal Confidential Data (PCD) should be governed by clear and transparent procedures that satisfy the requirements of law and guidance and regulate working practices in both the disclosing and receiving organisations. In some circumstances these procedures and the underpinning standards should be set out within an agreed information sharing agreement (ISA) or protocol.

The CCG will ensure that, where it holds PCD with a clear legal basis to do so, the data will be shared with registered and regulated health and social care professionals who have a legitimate relationship with the individual for the purposes of direct patient care. Further information on the Caldicott 2 review (*to share or not to share*) can be found on the NHS Digital (formerly HSCIC) website: http://www.hscic.gov.uk/article/3638/Personal-data-access-FAQs

9. Year on Year Improvement Plan and Assessment

An assessment of compliance of requirements within the Information Governance Toolkit will be undertaken each year. The results of the return will be monitored along with any action / development plan by the Information Governance Steering Group. The Information Governance Steering Group via the Information Governance Lead will report on the progress of the CCG against the Action Plan and Toolkit to the Quality Committee. The annual assessment will be submitted to the Governing Body for ratification. The requirements are grouped into the following initiatives:

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

10. Effective Safety Culture

The CCG encourages and promotes an effective safety culture throughout the organisation.

An effective safety culture:

- Sees errors as learning opportunities
- Motivates individuals to talk and be 'open' about their own experiences by encouraging such experiences to be shared
- Responds to problems that are identified
- Does not unfairly 'penalise' those who have made errors
- Has a reporting system that is seen to uncover the underlying causes of incidents
- Staff should feel at ease when reporting any incident/s that either do, or could potentially threaten information security. Examples of such incidents are as follows:-
- Using another user's login id / swipe card
- Unauthorised disclosure of information
- Leaving confidential / sensitive files out
- Theft or loss of IT equipment
- Theft or loss of computer media, that is floppy disks or memory sticks
- Accessing a person's record inappropriately for example viewing your own health record or family members, neighbours, friends and so on.
- Writing passwords down and not locking them away
- Identifying that a fax has been sent to the wrong recipient
- Sending / receiving a sensitive e-mail to / from "all staff" by mistake
- Giving out or overhearing personally identifiable information over the telephone
- Positioning of pc screens where information could be viewed by the public
- Software malfunction
- Inadequate disposal of confidential material (placed into a general wastebin)

Whilst the CCG, as an organisation is eager to avoid a 'blame culture' becoming embedded in any way, staff should be mindful that any staff member found to deliberately, recklessly or negligently breaching confidentiality may be subject to disciplinary action (including dismissal), face legal proceedings or both dependent on the seriousness of the incident.

11. Audit and Monitoring Compliance

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

IG Toolkit

Overall compliance with this framework will be reviewed annually through review arrangements for IG required by the IG Toolkit and reported to the CCG Quality Committee and Governing Body.

IG Incidents

The IG Steering Group has responsibility for providing assurances that this framework is adequate for providing clear guidance in the event of significant changes which may affect the framework. The designated IG Manager will ensure that adequate arrangements exist for:

- Reporting incidents, Caldicott issues
- Analysing and upward reporting of incidents and adverse events
- Reporting IG work programs and progress reports
- Reporting Information Governance Toolkit (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 as a 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.

12. Dissemination and Implementation

The policy will be published on the intranet and staff shared drive. Managers are required to ensure that their staff understand its application to their practice. Awareness of any new content or change in process will be through electronic channels for example through e-mail, in bulletins and so on.

Where a substantive revision is made then a separate plan for communicating and implementing this change will be devised by the SIRO.

13. Training

All staff likely to be in post 3 months or longer (permanent, temporary, contracted or seconded) are required to complete the online mandatory IG training modules (https://www.igtt.hscic.gov.uk/igte/index.cfm) within one month of joining, with further training required for managers / team leaders, staff who process personal information, and staff with specific information roles. A Training Needs Analysis (TNA) has been developed for staff in key roles, as part of effective delivery of training program.

However, should staff have access to personal identifiable information; training should be completed within 1 week, regardless of intended service length.

14. Related Documents

The following documentation relates to the management of information and together underpins the CCG's Information Governance Assurance Framework. This policy should be read in conjunction with other policies:

- Data Protection & Confidentiality Policy
- Safe Haven Policy
- Information Lifecycle Management Policy & Strategy
- Information Sharing Policy
- Information Risk Policy
- Forensic Readiness Policy
- Access to Information Policy
- Privacy Impact Assessment Policy
- Acceptable Use of Electronic Communications Policy
- Information Security Policy
- Information & Cyber Security Policy
- IG Management Framework

Legal Acts Covered Under This Policy:

- Data Protection Act 1998
- Human Rights Act 1998

- Freedom of Information Act 2000
- Access to Health Records Act 1990 (Where not superseded by the Data Protection Act 1998)
- Computer Misuse Act 1990
- Copyright, designs and patents Act 1988 (as amended by the Copyright Computer Programs Regulations 1992)
- Crime and Disorder Act 1998
- Electronic Communications act 2000
- Regulations of Investigatory Powers Act 2000

15. Equality and Diversity

The CCG recognises the diversity of the local community and those in its employment. The CCG aims 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 document has been assessed for equality impact on the protected groups, as set out in the Equality Act 2010.

This policy is applicable to every member of staff within the CCG irrespective of their age, disability, sex, gender reassignment, pregnancy, maternity, race (which includes colour, nationality and ethnic or national origins), sexual orientation, religion or belief, marriage or civil partnership.

16. Key Contacts

Within the CCG

Senior Information Risk Owner	Chief Officer – Sam Hepplewhite
Caldicott Guardian	Director of Nursing and Clinical Quality – Lisa Llewelyn
CCG IG Champion	Business Systems and Development Manager – Laura Ellis

Information Governance Team

Jane Marley	Head of Information Governance	jane.marley@nhs.net
Tracey Van Wyk	IG Lead	tracey.vanwyk@nhs.net

Iain Gear	FOI Lead	iain.gear@nhs.net
Debbie Smith-Shaw	Information Governance Adviser	Debbie.smith-shaw@nhs.net