Information Governance Policy

DOCUMENT CONTROL

<table>
<thead>
<tr>
<th>Version:</th>
<th>0.2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ratified By:</td>
<td></td>
</tr>
<tr>
<td>Date Ratified:</td>
<td></td>
</tr>
<tr>
<td>Policy Author:</td>
<td>Essex CSU CCG IG Lead</td>
</tr>
<tr>
<td>Policy Sponsor:</td>
<td>Senior Information Risk Owner (SIRO)</td>
</tr>
<tr>
<td>Name of Responsible Committee:</td>
<td>Quality and Governance Committee</td>
</tr>
<tr>
<td>Date Issued:</td>
<td></td>
</tr>
<tr>
<td>Review Date:</td>
<td></td>
</tr>
<tr>
<td>Target Audience:</td>
<td>CCG Staff and Members</td>
</tr>
</tbody>
</table>

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.
Associated Policy Documents

<table>
<thead>
<tr>
<th>Reference</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Data Protection and Confidentiality Policy</td>
</tr>
<tr>
<td></td>
<td>Information Security Policy</td>
</tr>
<tr>
<td></td>
<td>Safe Haven Policy</td>
</tr>
<tr>
<td></td>
<td>Freedom of Information Policy</td>
</tr>
<tr>
<td></td>
<td>Information Sharing Policy</td>
</tr>
<tr>
<td></td>
<td>Information Lifecycle Management Policy and Strategy</td>
</tr>
<tr>
<td></td>
<td>Information Risk Policy</td>
</tr>
<tr>
<td></td>
<td>Registration Authority Policy</td>
</tr>
</tbody>
</table>

Glossary

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>CCG</td>
<td>Clinical Commissioning Group</td>
</tr>
<tr>
<td>CSU</td>
<td>Commissioning Support Unit</td>
</tr>
<tr>
<td>CQRS</td>
<td>Calculating Quality Reporting System</td>
</tr>
<tr>
<td>IG</td>
<td>Information Governance</td>
</tr>
<tr>
<td>FOIA</td>
<td>Freedom of Information Act</td>
</tr>
<tr>
<td>DPA</td>
<td>Data Protection Act</td>
</tr>
<tr>
<td>GPES</td>
<td>General Practice Extraction Service</td>
</tr>
<tr>
<td>IGT</td>
<td>Information Governance Toolkit</td>
</tr>
<tr>
<td>IGTT</td>
<td>Information Governance Training Tool</td>
</tr>
<tr>
<td>ISA or ISP</td>
<td>Information Sharing Agreement or Protocol</td>
</tr>
<tr>
<td>SIRO</td>
<td>Senior Information Risk Owner</td>
</tr>
</tbody>
</table>
1. **Contents**

1. Contents........................................................................................................................................... 4

2. Introduction ........................................................................................................................................ 5

3. Purpose of Policy ................................................................................................................................ 5

4. Scope .................................................................................................................................................. 5

5. Principles ............................................................................................................................................. 6

6. Responsibilities of the CCG ................................................................................................................. 6

7. Responsibilities of Individuals ................................................................................................................ 7

8. Information Governance Framework ................................................................................................... 7
   8.1 Information Governance Management ......................................................................................... 8
   8.2 Confidentiality & Data Protection ................................................................................................. 8
   8.3 Information Security Assurance ..................................................................................................... 9
   8.4 Clinical & Corporate Information Assurance .............................................................................. 9
   8.5 Secondary Use Assurance ............................................................................................................. 9

9. Information Sharing .............................................................................................................................. 10

10. Year on Year Improvement Plan and Assessment ............................................................................ 11

11. Training .............................................................................................................................................. 11

12. Monitoring .......................................................................................................................................... 12

13. Effective Safety Culture ...................................................................................................................... 12

14. Legal Acts Covered Under This Policy ............................................................................................. 13

15. Key Contacts within the CCG ............................................................................................................ 13
2. Introduction

Information is a vital asset; Castle Point and Rochford CCG (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/Connecting for Health Information Governance Toolkit. It will do this with management accountability and structures and by providing a robust governance framework for information management.

3. Purpose of Policy

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, non-executive directors, 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 extranet 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.

4. Scope

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

- Patient/Client/Service User Information
- Staff Information
- Organisational Information

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

- Structured record systems (Including clinical) – paper and electronic

Policy Ref:
Version: 0.2
Approved
Review date
• 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.

5. 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 its public accountability, but equally places importance on the confidentiality of, and the security arrangements to safeguard, both personal information about patients and staff and information of a commercially sensitive nature. The CCG also recognises the need to share patient information with other health and social care organisations and other agencies, legally, and in a controlled and consistent manner, with the interests of the patient 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 information effectively in decision making processes.

6. Responsibilities of the Clinical Commissioning Group (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.

Patient’s 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.

7. Responsibilities of Individuals

The SIRO has overall responsibility for the implementation and delivery of the DPA 1998, on behalf of the CCG with devolved responsibility to the Information Governance Lead.

The SIRO is responsible for facilitating the implementation of the policy and supporting CCG staff to understand their responsibilities.

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

8. Information Governance Framework

Information will be defined and where appropriate kept confidential, underpinning the principles of Caldicott 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 health care, options for treatment available and their rights as patients 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 framework 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, Freedom of Information Act 2000 and the common law duty of confidentiality.

Awareness and understanding of all staff, with regards to their responsibilities, will be routinely assessed and appropriate training and awareness provided through staff 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.

8.1 Information Governance Management

Information Governance Management across the CCG will be co-ordinated by the Essex CSU Information Governance Team via the Information Governance Steering Group, which is accountable to the CCG’s Quality and Governance Committee.

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

- Recommending for approval, by the CCG Board, related policies and procedures
- Recommending for approval to the CCG Management Team the annual submission of compliance with the requirements for the Information Governance Toolkit and related action plan
- To co-ordinate and monitor the Information Governance Agenda across the CCG

8.2 Confidentiality & Data Protection

- The CCG will appoint 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 appoint a Senior Information Risk Owner (SIRO) to lead on the Management of all Risks.

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.

8.3 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.

8.4 Clinical & 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.
- 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 Board 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 Board.

8.5 Secondary Use Assurance

- The CCG will ensure that NHS standard definitions, values and validation programmes are incorporated within key systems.
- The CCG will ensure that, it monitors and improves data quality.

- The CCG will work with the Health and Social Care Information Centre to fulfil its obligations, with regards to carrying out in relation to encouraging information sharing for purposes of research using new initiatives such as GPES and CQRS.
However patient confidentiality shall remain of paramount importance to the CCG.

- The CCG will use local and national benchmarking to identify possible data quality issues and analyse trends in information
- The CCG will work with its main commissioning partners to assure itself of the validity of the CCG’s data
- The CCG will engage fully with the Audit Commission’s Payment by Results (PbR) data assurance framework

9.0 Information Sharing

The sharing of confidential patient-identifiable information 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 may need to share confidential patient-identifiable information with a range of organisations. The purposes to be served by sharing information will either relate to the provision of care, including the quality assurance of that care, for the individual concerned or will be for non-care or secondary purposes e.g. service evaluation, patient complaints or care enquiries, research, finance, public health work etc.

Information sharing protocols can be a useful way of providing a transparent and level playing field for organisations that need to exchange information. They can provide assurance in respect of the standards that each party to an agreement will adopt. However, they do not in themselves provide a lawful basis for sharing confidential information. This can only be achieved from effectively informing patients about the possibility of sharing and the choices they have available to them, to limit sharing. If the patient says ‘no’ to sharing, then information may only be shared in exceptional circumstances. It is consent that determines whether information can be shared – with consent you don’t need an information sharing agreement for sharing to be lawful, without consent an agreement is meaningless.

Information partners can be, but are not limited to:

- Other NHS Organisations
- Social Care and other Local Authority elements
- The Police
- Education Services
- Voluntary Sector Providers
- Private Sector Providers
The CCG will identify its non-NHS information partners and begin a process to understand and document the information requirements of each partner.

Having identified all its non-NHS information partners and the business needs served by exchanging information, the CCG will develop a high-level protocol that sets out the basic information governance principles agreed with each organisation. This high level protocol will be augmented by specific sections which apply to each information-sharing partner, so that the CCG has appropriate information sharing protocols agreed with all of its main non-NHS information-sharing partners.

All information sharing protocols will be regularly reviewed and updated. The identification, documentation and protocols for sharing patient-identifiable information will be agreed with all new information-sharing partners, prior to any exchange of information taking place.

Please refer to the CCG Information Sharing Policy for specific guidance on the procedure for information sharing.

10. 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 CSU IG Lead will report on the progress of the CCG against the Action Plan and Toolkit to the Quality and Governance Committee. The annual assessment will be submitted to the Board 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

11. IG Training

All staff must complete, as part of their corporate induction, a brief introductory training session on information governance. At a later date, (usually within 3 months from start date) all staff will complete approved information governance training, varying dependent on the specifics of assigned job roles. All staff must complete, annually mandatory information governance training via one of the two approved methods;
i. Classroom style sessions co-ordinated by Essex CSU
ii. Role related, relevant module/s with the CfH Information Governance Training Tool (IGTT).

12. Monitoring

Compliance with this policy will be monitored through the use of spot checks of staff understanding/compliance and visits to sites. Any incidents reported using the CCG’s incident reporting process will be monitored to identify breaches to this policy and such incidents will be investigated.

13. 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, i.e. floppy disc or memory stick
- Accessing a person’s record inappropriately e.g. viewing your own health record or family members, neighbors, friends etc.,
- Writing passwords down and not locking them away
- Identifying that a fax has been sent to the wrong recipient
- Sending/receiving an sensitive email 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 waste-bin)

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 breach confidentiality may be subject to disciplinary action, (including dismissal) face legal proceedings, or both dependent on the seriousness of the incident.

14. Legal Acts Covered Under This Policy

- Data Protection Act 1998
- Human Rights Act
- Freedom of Information Act 2000
- Computer Misuse Act 1990
- Copyright, designs and patents Act 1988 (as amended by the Copyright Computer Programs Regulations 1992)
- Crime and Disorder Act
- Electronic Communications act 2000

15. Key Contacts within the CCG

Essex CSU IG Team – Jane Marley (jane.marley@nhs.net), Paul Cook (pcook3@nhs.net), Debbie Smith-Shaw (Debbie.smith-shaw@nhs.net), Gemma Kerr (gemmakerr@nhs.net)

Caldicott Guardian - Tricia D’Orsi

Senior Information Risk Owner – Victoria Gunn

CCG IG Lead – Michelle Angell
## Appendix A – Checklist for Approval of Policy

To be completed and attached to any document which guides practice when submitted to the appropriate committee for consideration and approval.

<table>
<thead>
<tr>
<th>Title of document being reviewed:</th>
<th>Yes/No/Unsure</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Title</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Is the title clear and unambiguous?</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Is it clear whether the document is a guideline, policy, protocol or standard?</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>2. Rationale</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Are reasons for development of the document stated?</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>3. Development Process</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Is the method described in brief?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Are people involved in the development identified?</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Do you feel a reasonable attempt has been made to ensure relevant expertise has been used?</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Is there evidence of consultation with stakeholders and users?</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>4. Content</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Is the objective of the document clear?</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Is the target population clear and unambiguous?</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Are the intended outcomes described?</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Are the statements clear and unambiguous?</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>5. Evidence Base</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Is the type of evidence to support the document identified explicitly?</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Are key references cited?</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Are the references cited in full?</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Are supporting documents referenced?</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>6. Approval</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Does the document identify which committee/group will approve it?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>If appropriate have the joint Human Resources/staff side</td>
<td>n/a</td>
<td></td>
</tr>
</tbody>
</table>

Policy Ref:  
Version: 0.2  
Approved  
Review date
<table>
<thead>
<tr>
<th>Title of document being reviewed:</th>
<th>Yes/No/Unsure</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>committee (or equivalent) approved the document?</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

7. **Dissemination and Implementation**

- Is there an outline/plan to identify how this will be done? 
- Does the plan include the necessary training/support to ensure compliance? **Yes**

8. **Document Control**

- Does the document identify where it will be held? 
- Have archiving arrangements for superseded documents been addressed?

9. **Process to Monitor Compliance and Effectiveness**

- Are there measurable standards or KPIs to support the monitoring of compliance with and effectiveness of the document? **Yes**
- Is there a plan to review or audit compliance with the document? **Yes**

10. **Review Date**

- Is the review date identified? **Yes**
- Is the frequency of review identified? If so is it acceptable? **Yes**

11. **Overall Responsibility for the Document**

- Is it clear who will be responsible for co-ordinating the dissemination, implementation and review of the documentation? **Yes**

12. **Equality Impact Assessment (EIA)**

- Has an equality analysis been undertaken in preparation for this policy? **Yes**
- Has the equality analysis been quality assured by the Equality and Diversity Group? 

**Individual Approval**

If you are happy to approve this document, please sign and date it and forward to the chair of the committee/group where it will receive final approval.

<table>
<thead>
<tr>
<th>Name</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Signature</td>
<td></td>
</tr>
</tbody>
</table>

Policy Ref:  
Version: 0.2  
Approved  
Review date
<table>
<thead>
<tr>
<th>Name</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Signature</td>
<td></td>
</tr>
<tr>
<td>Target Group for initial awareness or training</td>
<td>Training Method</td>
</tr>
<tr>
<td>-----------------------------------------------</td>
<td>----------------</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Policy Title:  
Policy Owner:  
Approving Committee:  
Group/committee responsible for ensuring actions are in place

<table>
<thead>
<tr>
<th>Aspect of the policy to be monitored</th>
<th>Monitoring Method</th>
<th>Individual/Team responsible for the monitoring</th>
<th>Frequency</th>
<th>Group/committee that will receive the findings/monitoring report</th>
<th>Actions taken by the Group/committee</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>