Newcastle Gateshead
Clinical Commissioning Group

NHS Newcastle Gateshead Clinical Commissioning Group

Information Governance Strategy

Document Status	**Final**
Equality Impact Assessment	**No impact**
Document Ratified/Approved By	**Quality, Safety & Risk Committee Nov 2018**
Date Issued	**November 2018**
Date To be Reviewed	**November 2020**
Distribution	**All Staff**
Author	**Senior Governance Manager, North of England CSU**
Version	**2**
Reference No	**ISG01**
Location	**CCG Website**

1. INTRODUCTION

1.1 Information is a vital asset within the CCG, in terms of the effective commissioning and management of services and resources. It plays a key part in clinical governance, service planning and performance management. It is important that information is processed within a framework that ensures it is appropriately managed and that policies, procedures, management accountability and structures are in place.

1.2 This strategy sets out the approach to be taken within the CCG to provide a robust Information Governance (IG) framework and to fulfil its overall objectives and legislative requirements. Good IG ensures that best practice is implemented and on-going awareness is evident across the CCG. The CCG is committed to ensuring that all records and information are dealt with legally, securely, efficiently and effectively.

1.3 IG is a framework for handling information in a confidential and secure manner to appropriate ethical, quality and legislative standards. This IG strategy brings together within a cohesive framework, the interdependent requirements and standards of practice. It is defined by the requirements within the Data Security and Protection (DSP) Toolkit against which the CCG is required to publish an annual self-assessment of compliance. This strategy will be supported by a DSP Toolkit Action Plan.

1.4 The IG agenda encompasses the following areas:

- Caldicott
- NHS Confidentiality Code of Practice
- *Data Protection Act 2018*
- *Freedom of Information Act 2000*
- *Health and Social Care Act 2012*
- *Human Rights Act 1998*
- *Care Act 2014*
- General Data Protection Regulations
- Records Management (Health, Business and Corporate)
- Information Security
- Information Quality
- Confidentiality
- Openness
- Legal Compliance
- Information Risk

1.5 Within this agenda the CCG will handle and protect many classes of information:

- Some information is confidential because it contains personal details. The CCG must comply with regulations governing the processing and/or sharing of confidential personal information. Changes to the way in which patient confidential data can be processed came about as a result of the Health and Social Care Act 2012. It is important that relevant, timely and accurate information is available to those who are involved in the care of service users, but it is also important that personal information is not shared more widely than is necessary.
- Some information is non-confidential and is for the benefit of the CCG and the general public. The CCG and its employees share responsibility for ensuring that this type of information is accurate, up to date and easily accessible to the public.
- The majority of information about the CCG and its business should be open to public scrutiny although some, which is commercially sensitive, may need to be safeguarded.

1.6 Information can be in many forms, including (but not limited to):

- Structured record systems – paper and electronic
- Transmission of information – fax, e-mail, post and telephone; and
- All information systems purchased, developed and managed by/or on behalf of the organisation

2. PURPOSE

2.1 The IG arrangements will underpin the CCG's strategic goals and ensure that the information needed to support and deliver their implementation is readily available, accurate and understandable. IG has four fundamental aims:

- To support the provision of high quality care by promoting the effective and appropriate use of information
- To encourage all staff to work closely together, preventing duplication of effort and enabling efficient use of resources
- To provide staff with appropriate tools and support to enable them to carry out their responsibilities to consistently high standards
- To enable the CCG to understand its own performance and manage improvement in a systematic and effective manner
- To ensure full compliance with legislation relevant to IG and to enforce the rights of data subjects under the Data Protection Act 2018.

3. STRATEGIC AIMS

3.1 The strategic aims will be achieved by ensuring the effective management of IG by:

- Ensuring that the CCG meets its obligations under the Data Protection Act 2018 (including the General Data Protection Regulations), the Human Rights Act 1998, the Freedom of Information Act 2000 and the Health and Social Care Act 2012.
- Ensuring that effective action planning (with the support of the NECS IG service) is in place during 2018/19 – 2019/20 so that the CCG is GDPR compliant in 2018 and beyond.
- Establishing, implementing and maintaining policies for the effective management of information.
- Ensuring that IG is a cohesive element of the internal control systems within the CCG.
- Recognising the need for an appropriate balance between openness and confidentiality in the management of information.
- Ensuring that IG is an integral part of the CCG culture and its operating systems.
- Ensuring full compliance with the mandatory elements of the DSP Toolkit.
- Reducing duplication and looking at new ways of working effectively and efficiently.
- Minimising the risk of breaches of personal data.
- Minimising inappropriate uses of personal data.
- Ensuring that Service Level Agreements and Data Sharing Agreements between the CCG and other organisations are managed and developed in accordance with IG principles.
- Ensuring that contracted bodies are monitored against IG standards and that existing contracts are GDPR compliant.
- Protecting the services, staff, reputation and finances of the CCG through the process of early identification of information risks and where these risks are identified ensuring sufficient risk assessment, risk control and elimination are undertaken.
- Ensuring there is provision of sufficient training, instruction, supervision and information to enable all employees to operate effectively within IG requirements.

4. ROLES AND RESPONSIBILITIES

4.1 The CCG has developed clear lines of accountability with defined responsibilities and objectives. The Quality, Safety & Risk Committee is chaired by a CCG Lay member has responsibility for overseeing the implementation of this strategy.

4.2 The Governing Body and has responsibility for overseeing the Governance agenda and receives assurance on governance and risk management, IG, research governance and quality and diversity issues.

4.3 The Chief Officer has overall accountability and responsibility for IG across the CCG and is required to provide assurance, through the Annual Governance Statement, that all risks to the CCG are mitigated.

4.4 The Senior Information Risk Owner (SIRO) holds responsibility for ensuring that information is processed and held securely throughout the CCG. The role covers all the aspects of information risk, the confidentiality of patient and service user information and information sharing. The DSP Toolkit sets out clear responsibilities of the SIRO in relation to risks surrounding information and information systems, which also extend to business continuity and the role of Information Asset Owners.

4.5 The Caldicott Guardian has an advisory role and is responsible for ensuring that the principles of confidentiality and data protection set out in the Caldicott Guidelines and the Data Protection Act are implemented.

4.6 IG expertise will be provided by the Senior Governance Manager (IG) and the Senior Governance Officer (IG), NECS, who will liaise directly with the responsible person within the CCG.

4.7 The Data Protection Officer (DPO) is a role required within GDPR under the Data Protection Act 2018. The CCG's DPO is the Senior Governance Manager (IG), NECS who will assist the CCG to monitor internal compliance, inform and advise on data protection obligations, provide advice regarding Data Protection Impact Assessments (DPIAs) and act as a contact point for data subjects and the supervisory authority.

5. RISK REGISTER

5.1 All IG risks are captured in the Safeguard Incident and Risk Management System (SIRMS).

5.2 All risks registered include actions and timescales identified to minimise the risks.

5.3 All risks (including IG risks) are reviewed by the Audit Committee as a standing agenda item.

6. INCIDENT REPORTING

6.1 Staff will need to comply with the CCGs Incident Reporting and Management Policy which provides detailed advice on the reporting and handling of incidents. This policy requires that all incidents are reported and that lessons learned will be shared across the organisation via a quarterly IG incident update.

6.2 Specifically, the CCG wishes to foster a culture of openness and learning, and staff are encouraged to be open about raising problems.

6.3 Incidents will be recorded and analysed using SIRMS and the impact of an incident will be graded according to the matrix together with the likelihood of occurrence or recurrence.

6.4 The General Data Protection Regulations (GDPR)/UK Data Protection Act 2018 imposes legal obligations on controllers to comply with the requirement to report specific breaches to the Information Commissioner's Office without undue delay and no later than 72 hours of becoming aware of such a breach, where the breach is likely to result in a risk to the rights and freedoms of individuals. As a guide, an IG serious incident could be any incident which involves actual or potential failure to meet the requirements of the Data Protection Act 2018 and/or the Common Law of Confidentiality. This includes, for example, unlawful disclosure or misuse of confidential data, recording or sharing of inaccurate data, information security breaches and inappropriate invasion of people's privacy.

6.5 Incidents will be assessed and reported in accordance with NHS Digital's Guide to the Notification of Data Security and Protection Incidents within the DSP Toolkit and will be either reportable or not reportable via the DSP Toolkit. A reportable incident is one which meets the 'reportable' criteria following use of the Breach Assessment Grid within the guidance.

6.6 In most cases a reportable incident is investigated by the organisation where it occurred, however the responsibility for the incident will rest with the data controller. Where appropriate, regulatory bodies will be informed, for example the Information Commissioner's Office in connection with reportable Data Security & Protection incidents.

6.7 Serious Incidents will also be recorded and analysed using SIRMS and the impact of an incident will be graded according to the matrix. The Breach Assessment Grid within the NHSD guidance will be used to assess the severity of an incident and whether it is to be reported via the DSP Toolkit.

6.8 Incidents are reviewed by the Quality, Safety and Risk Committee and Audit Committee via quarterly governance reports.

6.9 Reportable incidents are reviewed by the Quality, Safety and Risk Committee.

7. TRAINING AND AWARENESS

7.1 Training and education are key to the successful implementation of this Strategy and embedding a culture of IG management in the organisation. Staff will have the opportunity to develop more detailed knowledge and appreciation of the role of IG through:

- Policy/strategy
- Induction
- Line manager
- Specific training courses
- Statutory and Mandatory training workshops
- Information Asset Administrator and Information Asset Owner workshops
- Communications/updates from the IG Lead

7.2 Mandatory training sessions will be delivered online via the NHS Digital (formerly the Health and Social Care Information Centre) Data Security Level 1 e-learning package. These sessions are mandatory and must be completed every year. Data Security Standard 3 within the Caldicott 3 review requires that all staff undertake appropriate annual data security training and pass a mandatory test. Therefore, non-permanent staff must also complete annual training.

7.3 Awareness will be monitored via regular checks and gaps in knowledge will be addressed via further bespoke training materials and/or targeted training sessions provided by the NECS IG service.

8. DISSEMINATION AND IMPLEMENTATION

8.1 The Strategy will be circulated to all individuals identified with specific responsibilities and will be communicated to all staff and stakeholders by the most appropriate means. The Strategy will be published on the CCGs intranet site accessible by all CCG staff. All line managers are required to share the contents of this Strategy with their staff.

8.2 The implementation of this Strategy is reflected through the completion of the DSP Toolkit and the confirmation of all mandatory assertions therein. It is also supported by a detailed reporting structure through the CCG's committees which are described in the Strategy. Directors and senior leads will be responsible for ensuring the Strategy is implemented in their areas of responsibility.

9. MONITORING

9.1 Data Security and Protection Toolkit

9.1.1 The annual release of a new version of the Toolkit generally takes place in June / July. An updated action plan for improving and implementing the requirements of the toolkit will be submitted to the Executive Committee each year following release and consideration of the new version.

9.1.2 Monitoring reports will be routinely submitted to the Quality, Safety & Risk Committee. The CCG's progress will be reported to the Governing Body at regular intervals by the SIRO. The action plan and monitoring will be maintained by the CCG's Information Governance Officer, NECS.

9.1.3 The CCG will comply with the NHS Digital deadlines for submission of updates and the final assessment.

9.1.4 Annual IG performance will be summarised in the IG Annual Report to be presented to Executive Committee.

9.1.5 An internal audit of the DSP Toolkit will take place in quarter 4 as part of the CCG's internal audit plan.

9.1.6 The CCG's IG Lead will meet on a quarterly basis (or more regularly if required) with allocated IG contacts at NECS to review milestones and to check progress against agreed internal deadlines for DSP Toolkit completion and to provide evidence for upload.

9.1.7 A GAP report will be provided by the NECS IG Team in December of each year to highlight any areas within the Toolkit which need the CCG's attention in order to meet the Toolkit deadline of 31st March.

9.1.8 Internal deadlines for submission of evidence have been set at December each year allowing the final three months to be used to review, finalise and improve the information in the toolkit between January - April.

10. PERFORMANCE INDICATORS

10.1 The DSP Toolkit submission is a mandatory annual return; the criteria for compliance are set out within the Toolkit. The successful implementation of IG across the organisation will be reflected in a compliant Toolkit submission.

11. ASSOCIATED DOCUMENTS

11.1 The documents listed below have all been approved by the CCG:-

- Information Governance and Information Risk Policy
- Confidentiality and Data Protection Policy
- Information Security Policy
- Information Access Policy
- Data Quality Policy
- Records Management Policy and Strategy
- Social Media Policy
- Internet and Email Acceptable Use policy
- Business Continuity Plan
- Incident Reporting and Management Policy
- Information Governance Management Framework
- Information Governance Staff Handbook
- Data Protection Impact Assessment SOP
- Subject Access and Subject Rights Request SOP

12. REVIEW

12.1 This strategy will be updated at least annually and in accordance with the following as and when required:

- legislative changes,
- good practice guidance,
- case law,
- significant incidents reported,
- new vulnerabilities, and
- changes to organisational infrastructure.

12.2 This Strategy will be received by the Quality, Safety & Risk Committee for formal approval.

13. EQUALITY AND DIVERSITY STATEMENT

13.1 The CCG is committed to promoting human rights and providing equality of opportunity; not only in employment practices, but also in the way services are commissioned. The CCG also values and respects the diversity of its employees and the communities it serves. In applying this policy, the organisation will have due regard for the need to:

- Promote human rights
- Eliminate unlawful discrimination
- Promote equality of opportunity
- Provide for good relations between people of diverse groups

13.2 This Strategy aims to be accessible to everyone regardless of age, disability (physical, mental or learning), gender (including transgender), race, sexual orientation, religion/belief or any other factor which may result in unfair treatment or inequalities in health or employment.

13.3 Throughout the development of this Strategy the CCG has sought to promote equality, human rights and tackling health inequalities by considering the impacts and implications when writing and reviewing the strategy. The impact of this strategy is subject to an on-going process of review which is closed by the formal Equality Impact Assessment when the strategy is due to be reviewed.

13.4 Equality impact assessment

13.4.1 In accordance with equality duties an Equality Impact Assessment has been carried out on this strategy. There is no evidence to suggest that the strategy would have an adverse impact in relation to race, disability, gender, age, sexual orientation, religion and belief or infringe individuals' human rights.

Appendix A

Equality Impact Assessment

North of England Commissioning Support

Partners in improving local health

An Equality Impact Assessment (EIA) is a process of analysing a new or existing service, policy or process. The aim is to identify what is the (likely) effect of implementation for different groups within the community (including patients, public and staff).

We need to:

- Eliminate unlawful discrimination, harassment and victimisation and other conduct prohibited by the Equality Act 2010
- Advance equality of opportunity between people who share a protected characteristic and those who do not
- Foster good relations between people who share a protected characteristic and those who do not

This is the law. In simple terms it means thinking about how some people might be excluded from what we are offering.

The way in which we organise things, or the assumptions we make, may mean that they cannot join in or if they do, it will not really work for them.

It's good practice to think of all reasons why people may be excluded, not just the ones covered by the law. Think about people who may be suffering from socio-economic deprivation or the challenges facing carers for example.

This will not only ensure legal compliance, but also help to ensure that services best support the healthcare needs of the local population.

Think of it as simply providing great customer service to everyone.

As a manager or someone who is involved in a service, policy, or process development, you are required to complete an Equality Impact Assessment using this toolkit.

Policy	A written statement of intent describing the broad approach or course of action the Trust is taking with a particular service or issue.
Service	A system or organisation that provides for a public need.
Process	Any of a group of related actions contributing to a larger action.

STEP 1 - EVIDENCE GATHERING

Name of person completing EIA:	**Alan Clement**
Title of service/policy/process:	**Information Governance Strategy 2018/19 – 2019/20**

Existing: ☐ **New/proposed:** ☐ **Changed:** √

What are the intended outcomes of this policy/service/process? Include outline of objectives and aims

This Strategy sets out:

- **the approach and arrangements for the management of information governance within the CCG**
- **the approach to information governance in our role as a Clinical Commissioning Group**

Who will be affected by this policy/service /process? (please tick)

☐ **Consultants** ☐ **Nurses** ☐ **Doctors**
√ **Staff members** ☐ **Patients** ☐ **Public**
√ **Other**

If other please state:

What is your source of feedback/existing evidence? (please tick)

☐ **National Reports** ☐ **Internal Audits**
☐ **Patient Surveys** ☐ **Staff Surveys** ☐ **Complaints/Incidents**
☐ **Focus Groups** ☐ **Stakeholder groups** ☐**Previous EIAs**
√ **Other**

If other please state:
The IG Strategy is guided by legislation and national requirements.

Evidence	What does it tell me? (about the existing service/policy/process? Is there anything suggest there may be challenges when designing something new?)
National Reports	
Patient Surveys	
Staff Surveys	
Complaints and Incidents	
Results of consultations with different stakeholder groups – staff/local community groups	
Focus Groups	
Other evidence (please describe)	**The IG Strategy is driven by legislation, national strategy and guidance such as the DSP Toolkit and ICO best practice recommendations.**

STEP 2 - IMPACT ASSESSMENT

What impact will the new policy/system/process have on the following: (Please refer to the 'EIA Impact Questions to Ask' document for reference)
Age A person belonging to a particular age
None identified
Disability A person who has a physical or mental impairment, which has a substantial and long-term adverse effect on that person's ability to carry out normal day-to-day activities
None identified
Gender reassignment (including transgender) Medical term for what transgender people often call gender-confirmation surgery; surgery to bring the primary and secondary sex characteristics of a transgender person's body into alignment with his or her internal self-perception.
None identified
Marriage and civil partnership Marriage is defined as a union of a man and a woman (or, in some jurisdictions, two people of the same sex) as partners in a relationship. Same-sex couples can also have their relationships legally recognised as 'civil partnerships'. Civil partners must be treated the same as married couples on a wide range of legal matters
None identified
Pregnancy and maternity Pregnancy is the condition of being pregnant or expecting a baby. Maternity refers to the period after the birth, and is linked to maternity leave in the employment context.
None identified
Race It refers to a group of people defined by their race, colour, and nationality, ethnic or national origins, including travelling communities.
None identified
Religion or belief Religion is defined as a particular system of faith and worship but belief includes religious and philosophical beliefs including lack of belief (e.g. Atheism). Generally, a belief should affect your life choices or the way you live for it to be included in the definition.
None identified
Sex/Gender A man or a woman.
None identified
Sexual orientation Whether a person's sexual attraction is towards their own sex, the opposite sex or to both sexes
None identified
Carers A family member or paid helper who regularly looks after a child or a sick, elderly, or disabled person
None identified
Other identified groups such as deprived socio-economic groups, substance/alcohol abuse and sex workers
None identified

 **STEP 3** - ENGAGEMENT **AND INVOLVEMENT**

How have you engaged stakeholders in testing the policy or process proposals including the impact on protected characteristics?
Not applicable
Please list the stakeholders engaged:
Not applicable

 **STEP 4 - METHODS OF COMMUNICATION**

What methods of communication do you plan to use to inform service users of the policy?
□ **Verbal – stakeholder groups/meetings** □ **Verbal - Telephone** □ **Written – Letter** □ **Written – Leaflets/guidance booklets** □ **Email** □ **Internet** √ **Other**
If other please state: Not applicable to this type of internal strategy document.

ACCESSIBLE INFORMATION STANDARD

The Accessible Information Standard directs and defines a specific, consistent approach to identifying, recording, flagging, sharing and meeting the information and communication support needs of service users.

Tick to confirm you have you considered an agreed process for:
□ **Sending out correspondence in alternative formats.** □ **Sending out correspondence in alternative languages.** □ **Producing / obtaining information in alternative formats.** □ **Arranging / booking professional communication support.** □ **Booking / arranging longer appointments for patients / service users with communication needs.**
If any of the above have not been considered, please state the reason: Not applicable to this type of internal strategy document.

STEP 5 - SUMMARY OF POTENTIAL CHALLENGES

Having considered the potential impact on the people accessing the service, policy or process please summarise the areas have been identified as needing action to avoid discrimination.

Potential Challenge	What problems/issues may this cause?
None identified.	

STEP 6- ACTION PLAN

Ref no.	Potential Challenge/ Negative Impact	Protected Group Impacted (Age, Race etc.)	Action(s) required	Expected Outcome	Owner	Timescale/ Completion date
	N/A					

Ref no.	Who have you consulted with for a solution? (users, other services, etc.)	Person/ People to inform	How will you monitor and review whether the action is effective?
	N/A		

SIGN OFF

Completed by:	**Alan Clement**
Date:	**23rd August 2018**
Presented to: (appropriate committee)	**Quality, Safety & Risk Committee**
Publication date:	**November 2018**