Tees Valley
Clinical Commissioning Group

NHS Tees Valley Clinical Commissioning Group

Information Governance Strategy 2020/23

Document Status	Draft
Equality Impact Assessment	No impact Completed EIA (Appendix 1)
Document Ratified/Approved By	Audit & Assurance Committee Governing Body
Date Issued	April 2020
Date To be Reviewed	April 2023
Distribution	All Staff
Author	Senior Governance Manager, North of England CSU
Version	1
Reference No	IGS01

Contents

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 managed 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 Framework and to fulfil its overall objectives. Information Governance requirements ensure 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 Information Governance is "a framework for handling information in a confidential and secure manner to appropriate ethical and quality standards in modern health services". It brings together within a singular cohesive framework the interdependent requirements and standards of practice. It is defined by the requirements within the Data Security & Protection Toolkit (DSPT) against which the CCG is required to publish an annual self-assessment of compliance. This strategy is supported by a DSPT Action Plan.

1.4 The Information Governance 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 Regulation (GDPR)/ Records Management (Health, Business & 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 regulation which regulates the holding and 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 & 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 – 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 Information Governance 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. Information Governance has four fundamental aims:

- To support the provision of high quality care by promoting the effective and appropriate use of information
- To encourage responsible staff to work closely together, preventing duplication of effort and enabling efficient use of resources
- To develop support arrangements and 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

3. STRATEGIC AIMS

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

- Ensuring that the CCG meets its obligations under the Data Protection Act 2018, the Human Rights Act 1998, the Freedom of Information Act 2000 and the Health and Social Care Act 2012.
- Establishing, implementing and maintaining policies for the effective management of information
- Ensuring that information governance 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 information governance is an integral part of the CCG culture and its operating systems (Privacy by Design)
- Ensuring maintenance of year on year improvement within the DSPT self-assessment
- 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 Contracts, Service Level Agreements, Information Sharing Agreements and Data Processing Agreements between the CCG and other organisations are managed and developed in accordance with Information Governance Principles
- Ensuring that contracted bodies are monitored against Information Governance standards.
- 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 within information governance requirements
- Ensuring that information governance is embedded within the CCG and monitored via regular checks.
- Ensuring the CCG understands its processing activities including maintaining a record that details each use or sharing of personal information including the legal basis for the processing and if applicable, whether national data opt outs have been applied.
- Ensuring that a data security and protection breach reporting system is in place.

4. ROLES & RESPONSIBILITIES

4.1 The CCG has developed clear lines of accountability with defined responsibilities and objectives. The Audit and Assurance Committee is chaired by the governing body Lay Member and has responsibility for overseeing the implementation of this strategy.

4.2 The Audit and Assurance Committee is accountable to the Governing Body and has responsibility for overseeing and reporting to the Governing Body and providing assurance on Governance and Risk Management, Information Governance, Research Governance and Equality & Diversity issues.

4.3 The Chief Officer has overall accountability and responsibility for Information Governance 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 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 DSPT 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 legislation are implemented systematically.

4.6 The CCG is supported and advised by the Data Protection Officer (DPO) who assists the CCG to monitor internal compliance, informs and advises on our data protection obligations, provides advice regarding Data Protection Impact Assessments (DPIAs) and acts as a contact point for data subjects and the supervisory authority. The DPO for the CCG is the Senior Governance Manager (IG), North of England Commissioning Support Unit.

4.7 Information Governance expertise will be provided by the Senior Governance Manager (IG) and the Senior Governance Officer (IG), North of England Commissioning Support Unit, who will liaise directly with the responsible person within the CCG.

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 and Assurance Committee as a standing agenda item.

6. INCIDENT REPORTING

6.1 Staff will need to comply with the CCG's 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 Audit and Assurance Committee via quarterly governance reports.

6.9 Reportable incidents are reviewed by the Audit and Assurance 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
- The I.G. Handbook

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 CSU IG service.

8. MONITORING

8.1 Data Security and Protection Toolkit

8.1.1 An action plan for improving and implementing the requirements of the DSPT will be submitted to the Audit and Assurance Committee.

8.1.2 Monitoring reports will be routinely submitted to the Audit and Assurance 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 Senior Governance Officer (IG), North of England Commissioning Support Unit.

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

8.1.4 Annual IG performance will be summarised in the Information Governance Annual Report to be presented to the Audit and Assurance Committee.

8.1.5 An internal audit of the IG Toolkit is planned to take place in quarter 4 as part of the CCG's internal audit plan.

9. PERFORMANCE INDICATORS

9.1 The DSPT submission is a mandatory annual return; the criteria for compliance are set out within the DSPT. The successful implementation of Information Governance across the organisation will be reflected in the achievement level produced from the annual DSPT submission.

10. ASSOCIATED DOCUMENTS

10.1 This strategy should be read in conjunction with the following IG policies:-

- 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 and Instant Messaging Policy
- Internet and Email Acceptable Use policy
- Business Continuity Plan
- Incident Reporting and Management Policy
- Information Governance Staff Handbook
- Data Protection Impact Assessment SOP
- Subject Access and Subject Rights Request SOP

11. REVIEW

11.1 This strategy will be updated every three years and in accordance with the following as and when required:

- legislative changes
- as dictated by the DSP Toolkit
- good practice guidance;
- case law;
- significant incidents reported;
- new vulnerabilities; and
- changes to organisational infrastructure.

11.2 This Strategy will be received by the Audit and Assurance Committee for agreement prior to being received by the Governing Body for formal approval.

APPENDIX 1

necs Partners in improving local health

NHS North of England Commissioning Support Unit

Equality Analysis
Initial Screening Assessment

May 2019

Step 1

As a public body organisation we need to ensure that all our strategies, policies, services and functions, both current and proposed have given proper consideration to equality and diversity, do not aid barriers to access or generate discrimination against any protected groups under the Equality Act 2010 (Age, Disability, Gender Reassignment, Pregnancy and Maternity, Race, Religion/Belief, Sex, Sexual Orientation, Marriage and Civil Partnership, Carers and Health Inequalities).

A screening process can help judge relevance and provides a record of both the process and decisions made.

This screening determines relevance for all new and revised strategies, policies, projects, service reviews and functions.

Completed at the earliest opportunity it will help to determine:

- The relevance of proposals and decisions to equality, diversity, cohesion and integration.
- Whether or not equality and diversity is being/has already been considered for due regard to the Equality Act 2010 and the Public Sector Equality Duty (PSED).
- Whether or not it is necessary to carry out a full Equality Impact Assessment.

Name(s) and role(s) of person completing this assessment:

Name: Liane Cotterill Role: Senior Governance Manager, IG & DPO

Title of the service/project or policy:

Information Governance Strategy

Is this a:

X	Strategy / Policy		Service Review		Project

If other, please specify:

What are the aim(s) and objectives of the service, project or policy:

This strategy 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.

Who will the project/service /policy / decision impact?

Consider the actual and potential impacts:

- [x] Staff
- [ ] service users/patients
- [ ] other public sector organisations
- [ ] voluntary / community groups / trade unions
- [ ] others, please specify:

Questions	Yes	No
Could there be an existing or potential impact on any of the protected characteristic groups?		X
Has there been or likely to be any staff/patient/public concerns?		X
Could this piece of work affect how our services, commissioning or procurement activities are organised, provided, located and by whom?		X
Could this piece of work affect the workforce or employment practices?		X
Does the piece of work involve or have an impact on: • Eliminating unlawful discrimination, victimisation and harassment • Advancing equality of opportunity • Fostering good relations		X

If you have answered no to the above and conclude that there will not be a detrimental impact on any equality group caused by the proposed policy/project/service change, please state how you have reached that conclusion below:

The policy is based on the former NHS South Tees, NHS Hartlepool & Stockton on Tees and NHS Darlington CCGs' policy. There is no fundamental change to the content therefore the previous EIA which concluded 'no impact' remains appropriate.

If you have answered yes to any of the above, please now complete the 'STEP 2 Equality Impact Assessment' document.

Governance, ownership and approval

Please state here who has approved the actions and outcomes of the screening		
Name	**Job title**	**Date**
Liane Cotterill	Senior Governance Manager	February 2020

Publishing

This screening document will act as evidence that due regard to the Equality Act 2010 and the Public Sector Equality Duty (PSED) has been given.

If you are not completing 'STEP 2 - Equality Impact Assessment' this screening document will need to be approved and published alongside your documentation.

A copy of all screening documentation should be sent to: **NECSU.Equality@nhs.net** for audit purposes.