NHS
North East and North Cumbria

Corporate	ICBP023 Information Governance Strategy 2022-25

Version Number	Date Issued	Review Date
2	October 2022	October 2024

Prepared By:	Senior Governance Manager, NECS
Consultation Process:	Integrated Governance Workstream
Formally Approved:	October 2022
Approved By:	Executive Committee

EQUALITY IMPACT ASSESSMENT

Date	Issues
June 2022	None

POLICY VALIDITY STATEMENT

Policy users should ensure that they are consulting the currently valid version of the documentation. The policy will remain valid, including during its period of review. However, the policy must be reviewed at least once in every 3-year period.

ACCESSIBLE INFORMATION STANDARDS

If you require this document in an alternative format, such as easy read, large text, braille or an alternative language please contact NECSU.comms@nhs.net

Version Control

Version	Release Date	Author	Update comments
1	July 2022	Senior Governance Manager, NECS	First Issue
2.0	October 2022	Senior Governance Manager, NECS	Initial 6 monthly review following ICB establishment, no updates required

Approval

Role	Name	Date
Approver	Executive Committee	July 2022
Approver	Executive Committee	October 2022

Contents

1. INTRODUCTION

1.1 Information is a vital asset within the ICB, 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 ICB 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 ICB. The ICB 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 ICB 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
- National Health Service Act 2006
- 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 ICB will handle and protect many classes of information:

- Some information is confidential because it contains personal details. The ICB must comply with regulation which regulates the holding and sharing of confidential personal information. 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 ICB and the general public. The ICB 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 ICB 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 ICB'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 ICB 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 ICB meets its obligations under the Data Protection Act 2018, the Human Rights Act 1998, the Freedom of Information Act 2000 and the Health and Care Act 2022.
- 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 ICB
- 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 ICB 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 ICB 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 ICB 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 ICB and monitored via regular checks.

- Ensuring the ICB 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 ICB has developed clear lines of accountability with defined responsibilities and objectives. The Audit Committee is chaired by the ICB Board Non-Executive Member and has responsibility for overseeing the implementation of this strategy.

4.2 The Audit Committee is accountable to the ICB Board and has responsibility for overseeing and reporting to the Board and providing assurance on areas outlined within its terms of reference; this includes receiving regular updates on IG compliance and the Data Security and Protection Toolkit.

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

4.4 The SIRO holds responsibility for ensuring that information is processed and held securely throughout the ICB. 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 ICB is supported and advised by the Data Protection Officer (DPO) who assists the ICB to monitor internal compliance, informs and advises on 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 ICB 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 ICB.

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 and/or overseen by an ICB Board Committee, in line with Scheme of Reservation and Delegation and Terms of Reference.

6. INCIDENT REPORTING

6.1 Staff will need to comply with the ICB'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 ICB 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 Executive Committee via quarterly governance reports.

6.9 Reportable incidents are reviewed by the Executive Committee.

7. TRAINING AND AWARENESS

7.1 Overall accountability for procedural documents across the organisation lies with the ICB Board which has overall responsibility for establishing and maintaining an effective document management system, for meeting all statutory requirements and adhering to guidance issued in respect of procedural documents.

7.2 Overall responsibility for the Information Governance Strategy lies with the Executive Director of Corporate Governance, Communications and Involvement who has delegated responsibility for managing the development and implementation of information governance procedural documents.

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

7.4 Mandatory training sessions will be delivered online via the NHS Digital 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.

7.5 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 Committee.

8.1.2 Monitoring reports will be routinely submitted to the Audit Committee. The ICB's progress will be reported to the ICB Board 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 ICB 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 Committee.

8.1.5 The ICB will consider the auditing of the DSP Toolkit as part of its 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. DOCUMENTATION

10.1 Other related policy documents.

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

10.2 Legislation and Statutory Requirements

Care Act 2014
Data Protection Act 2018 (including UKGDPR)
Equality Act 2010
Freedom of Information Act 2000
General Data Protection Regulation 2016
Health and Care Act 2022
Human Rights Act 1998

10.3 Best Practice Recommendations

Caldicott Guardian Guidance
Common Law Duty of Confidentiality.

11. MONITORING, REVIEW AND ARCHIVING

11.1 **Monitoring**

The ICB Board will agree with the sponsoring director a method for monitoring the dissemination and implementation of this policy. Monitoring information will be recorded in the policy database.

11.2 **Review**

11.2.1 The ICB Board will ensure that this policy document is reviewed in accordance with the timescale specified at the time of approval. **No policy or procedure will remain operational for a period exceeding three years without a review taking place.**

11.2.2 Staff who become aware of any change which may affect a policy should advise their line manager as soon as possible. The sponsoring director will then consider the need to review the policy or procedure outside of the agreed timescale for revision.

11.2.3 For ease of reference for reviewers or approval bodies, changes should be noted in the 'document history' table on the front page of this document.

NB: If the review consists of a change to an appendix or procedure document, approval may be given by the sponsoring director and a revised document may

be issued. Review to the main body of the policy must always follow the original approval process.

11.3 Archiving

The ICB Board will ensure that archived copies of superseded policy documents are retained in accordance with the NHS Records Management Code of Practice 2021.

Schedule of Duties and Responsibilities

Through day to day work, employees are in the best position to recognise any specific fraud risks within their own areas of responsibility. They also have a duty to ensure that those risks, however large or small, are identified and eliminated. Where it is believed fraud, bribery or corruption could occur, or has occurred, this should be reported to Counter Fraud FS or the Executive Director of Finance immediately.

ICB Board	The ICB Board has responsibility for setting the strategic context in which organisational process documents are developed, and for establishing a scheme of governance for the formal review and approval of such documents.
Chief Executive	The Chief Executive has overall responsibility for the strategic direction and operational management, including ensuring that ICB process documents comply with all legal, statutory and good practice guidance requirements.
SIRO	The Senior Information Risk Owner (SIRO) holds responsibility for ensuring that information is processed and held securely throughout the organisation.
Caldicott Guardian	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 systematically
Commissioning Support Staff.	Whilst working on behalf of the ICB NECS staff will be expected to comply with all policies, procedures and expected standards of behaviour within the ICB, however they will continue to be governed by all policies and procedures of their employing organisation

All Staff	All staff, including temporary and agency staff, are responsible for: • Compliance with relevant process documents. Failure to comply may result in disciplinary action being taken. • Co-operating with the development and implementation of policies and procedures and as part of their normal duties and responsibilities. • Identifying the need for a change in policy or procedure as a result of becoming aware of changes in practice, changes to statutory requirements, revised professional or clinical standards and local/national directives, and advising their line manager accordingly. • Identifying training needs in respect of policies and procedures and bringing them to the attention of their line manager. • Attending training / awareness sessions when provided.

Appendix A – Equality Impact Assessment

Equality Impact Assessment
Initial Screening Assessment (STEP 1)

As a public body organisation we need to ensure that all our current and proposed strategies, policies, services and functions, have given proper consideration to equality, diversity and inclusion, 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).

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
Job Title: Senior Governance Manager, IG and DPO
Organisation: Click here to enter text.

Title of the service/project or policy: Information Governance Strategy

Is this a;
Strategy / Policy ☒ **Service Review** ☐ **Project** ☐
Other Click here to enter text.

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

This Strategy sets out •the approach and arrangements for the management of information governance within the ICB

Who will the project/service /policy / decision impact?
(Consider the actual and potential impact)

- **Staff** ☒
- **Service User / Patients** ☐
- **Other Public Sector Organisations** ☐

- **Voluntary / Community groups / Trade Unions** ☐
- **Others, please specify** Click here to enter text.

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

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 strategy is an annual review and has received only minor updates. 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

Accessible Information Standard	Yes	No
Please acknowledge you have considered the requirements of the Accessible Information Standard when communicating with staff and patients. https://www.england.nhs.uk/wp-content/uploads/2017/10/accessible-info-standard-overview-2017-18.pdf	☒	☐
Please provide the following caveat at the start of any written documentation: **"If you require this document in an alternative format such as easy read, large text, braille or an alternative language please contact (ENTER CONTACT DETAILS HERE)"**		
If any of the above have not been implemented, please state the reason: Click here to enter text.		

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 IG and DPO	July 2022

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.

Please send a copy of this screening documentation to: NECSU.Equality@nhs.net for audit purposes.