NHS
Sunderland
Clinical Commissioning Group

# Information Governance and Information Risk Policy

IG03

Better health for Sunderland

| Version | Date Approved | Committee | Date of next review | CCG Lead |
|---|---|---|---|---|
| 3 | 01/03/2016 | Executive Committee | January 2018 | Debbie Cornell |
| 3.1 | February 2018 | Executive Committee | May 2018 | Debbie Cornell |
| 4 | September 2018 | Executive Committee | September 2020 | Debbie Cornell |
| 5 | Sept 2020 | Executive Committee | April 2022 | Debbie Cornell |

## Equality Impact Assessment

| Date | Issues |
|---|---|
| August 2020 | See Section 10 |

**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.

# Contents

## 1. Introduction

The CCG aspires to the highest standards of corporate behaviour and clinical competence, to ensure that safe, fair and equitable procedures are applied to all organisational transactions, including relationships with patients, their carers, public, staff, stakeholders and the use of public resources. In order to provide clear and consistent guidance, the CCG will develop documents to fulfil all statutory, organisational and best practice requirements and support the principles of equal opportunity for all.

Information is a vital asset, both in terms of the management of health and social care for individual patients/service users and the efficient management of services and resources. It plays a key part in governance, service planning and performance management.

Information risk management is an essential component of information governance and is an integral part of good management practice. The intent is to embed information risk management in a practical way into business processes and functions.

Information risk must be managed in a robust way within work areas and not be seen as something that is the sole responsibility of IT or IG staff. A structured approach is needed, building upon the existing information governance framework and this approach relies upon the identification of information assets and assigning 'ownership' of assets to senior accountable staff.

It is therefore of paramount importance to ensure that information is efficiently managed including information risk, and that appropriate policies, procedures and management accountability provide a robust governance framework for information management. Information Governance (IG) is the means of providing this governance framework, and currently includes the following legislation and guidance:

- Data Protection Act 2018
- General Data Protection Regulations 2016
- Freedom of Information Act 2000
- Environmental Information Regulations 2004
- Access to Health Records Act 1990
- Department of Health Records Management: NHS Code of Practice for Health and Social Care 2016
- Computer Misuse Act 1990
- NHS Confidentiality Code of Practice
- Common Law Duty of Confidentiality
- Fraud Act 2006
- Further guidance on information governance legislation can be found in the Department of Health NHS Information Governance Guidance on Legal and Professional obligations.

The Framework sets out an overview of how the organisation is addressing the IG Agenda and the approach taken to ensure robust management of information. There are two key components underpinning the IG Framework;

- IG Policy which outlines the objective for information governance
- IG Strategy which details an overall plan arising from a baseline assessment against the requirements set out in the NHS Digital Data Protection and Security Toolkit.

The Data Protection and Security Toolkit consists of a series of evidence based requirements against which an organisation's current and planned attainment levels can be monitored. The organisation is required to complete an annual self-assessment against the Toolkit. The CCG Toolkit is broken down into ten National Data Guardian Standards:

- Personal Confidential Data
- Staff Responsibilities
- Training
- Managing Data Access
- Process Reviews
- Responding to Incidents
- Continuity Planning
- Unsupported Systems
- IT Protection
- Accountable Suppliers

## 1.1 Status

This policy is an Information Governance policy.

## 1.2 Purpose and scope

The purpose of this document is to present an Information Governance Policy & Information Risk Policy for the organisation. This sets out the organisation's commitment to the security, information risk management, confidentiality and quality of information. It also details how information governance and information risk will be managed within the organisation.

This policy is applicable to all employees, agents and contractors working for, or supplying services to the organisation. However, it is recognised that primary care practitioners are also part of the organisation and as such this policy is offered for use by them to adapt to their own practices and organisations as appropriate. The CCG is available to offer help and support to primary care practitioners who wish to use and implement this policy.

## 2. Definitions

The following terms are used in this document:

2.1 **Personal information** is factual information or expressions of opinion which relate to an individual who can be identified from that information or in conjunction with any other information coming into possession of the data holder. This also includes information gleaned from a professional opinion, which may rely on other information obtained. Personal information includes name, address, date of birth or any other unique identifiers such as NHS Number, Hospital Number, National Insurance Number, etc. It also includes information which, when presented in combination, may identify an individual e.g. postcode, date of birth etc.

2.2 **Sensitive information** also known as 'Special Category Data' as set out in the DPA 2018 is any information about a person relating to their;

- Racial or ethnic origin
- Political opinions
- Religious beliefs or other beliefs of a similar nature
- Trade union membership
- Biometric Data
- Physical or mental health or condition
- Sexual life
- Commission or alleged commission of any offence, or
- Any proceedings for any offence committed or alleged to have been committed

This type of data is subject to more stringent conditions on their processing when compared to 'personal information' (See 2.1).

2.3 **Information risk** is the chance of something happening to the information which will have an impact upon the objectives, personal safety and security of the organisation. Risk is determined in terms of consequence and likelihood and should be managed alongside other organisational risks and should be considered a fundamental component of effective information governance.

2.4 **Information Risk Management** is the culture, processes and structures that are directed towards the effective management of opportunities and adverse effects to information assets.

2.5 **Information assets** come in many shapes and forms and include:

- **Personal information** e.g. content within databases, archive and back up data, audit data, paper records (health, social care and staff records)
- **Software** e.g. application and system software, data encryption utilities, development and maintenance tools
- **Hardware** e.g. PCs, laptops, USB sticks, PDA
- **System/process documentation** e.g. system information and documentation, manual and training materials, contracts, business continuity plans policies, etc.

2.6 **Information Asset Register** is a record of all information assets along with the associated Information Asset Owner of each asset. Having an up to date and accurate IAR is a requirement under data protection legislation.

2.7 **Privacy by Design** means any action that involves processing personal data must be done with data protection and privacy in mind at every step. This includes internal projects, product development, software development, IT systems, and much more. In practice, this means that any department that processes personal data must ensure that privacy is built in to the whole life cycle of the process.

2.8 **Privacy by Default** means that once a product, process, or service has been introduced, the strictest privacy settings should apply by default, without any manual input from the end user. In addition, any personal data provided by the user should only be kept for the amount of time necessary to provide the service.

2.9 **Data Protection Impact Assessment** (DPIA) is a process to help you identify and minimise the data protection risks of a project. You must complete a DPIA for processing that is likely to result in a high risk to individuals. This includes some specified types of processing.

## 3. The Principles of Information Governance

3.1 Overview

3.1.1 There are a number of underlying principles governing Information Governance. An Information Governance Strategy will detail how these principles will be embedded throughout the organisation.

3.1.2 These principles can be divided into the different areas of information governance.

3.2 Information Governance Management

- There is a commitment to establish and maintain robust operational and management accountability structures, assign appropriate resources and dedicated staff to ensure that IG issues are dealt with appropriately, effectively and at levels within the organisation.
- There should be proactive use of information within and between the organisation, other NHS, and partner organisations to support patient/service user care as determined by law, statute and best practice
- There is a need for an appropriate balance between openness and confidentiality in the management and use of information
- There is a commitment to improving staff understanding of their responsibilities around information governance at a level relevant to their role
- There is a legal requirement to consider privacy by design when implementing any new or changed system or service being implemented
- There is a dedicated Information Governance component in the appropriate budget within the organisation.

3.3 Confidentiality and Data Protection Assurance

- There is a need to share patient/service user information with other health organisations and other non-health agencies in a controlled manner consistent with the interests of the patient/service user and, in some circumstances, the public interest.
- There should be effective arrangements to ensure confidentiality and security of personal and other sensitive information.
- There is a legal requirement to undertake Data Protection Impact Assessments for new processes, systems, projects etc.

3.4 Information Security Assurance

- There is a commitment to ensuring the security of all personal information held by the organisation through the implementation of policies, procedures and processes to ensure the confidentiality, integrity and availability of information
- There is a commitment to the implementation of security monitoring and audit processes to ensure compliance with key policy and procedures.
- There is a legal requirement to consider privacy by default when implementing systems and technologies.

3.5 Corporate Information Assurance

- There is a commitment to making non-confidential information widely available in line with responsibilities under FOI Act 2000 to ensure openness.
- There is a need for effective management of corporate paper and electronic records

3.6 Clinical Information Assurance

- There is a need for accurate, timely and relevant information in order to deliver the highest quality health and social care.
- There is a commitment to improving records management for care purposes in keeping with professional, legislative and statutory records management requirements

3.7 Secondary Use Assurance

- There is a commitment to developing quality data to support non-direct care related purposes (planning, commissioning, public health, finance)
- There is a commitment to improving data quality through the use of local and national benchmarking

## 4. Managing Information Risk

4.1 Introduction

4.1.1 The organisation places high importance on minimising information risk and safeguarding the interest of patients, staff and the organisation.

4.1.2 Information risk is inherent in all organisational activities and everyone working for, or on behalf of the organisation, has a responsibility to continuously manage information risk. The aim of information risk management is to provide the means to identify, prioritise and manage the risks involved in all of the organisation's activities.

4.2 Information Risk Management Assurance Framework

4.2.1 Information Risk Management Assurance Framework aims to:

- Protect patients, staff and the organisation from information risks where the likelihood of occurrence and the consequences are significant.
- Support the strategic approach to the risk management framework in which information risks will be identified, considered and addressed in the approval, review and control processes.
- Use the risk assessment methodology (risk matrix) to assess information risks e.g. threats to information.
- Encourage pro-active rather than re-active information risk management.
- Contribute to the quality of decision making throughout the organisation by supporting robust information.
- Meet legal or statutory requirements.
- Assist in safeguarding the organisation's information assets.

4.3 Assessment of Information Risk

4.3.1 The organisation will assess information risk in a number of ways, which will include the following:

- Routine review of flows of personal information to ensure any risks identified with these flows are mitigated, including ensuring appropriate controls are in place for data transferred outside the EEA.
- The organisation's risk management procedures provide clear guidance as to the way in which information risks and incidents are identified, assessed and managed across the organisation, and how the IG Risk Register supports this process. Investigating and learning from incidents will support the organisation in understanding the real level of risk being experienced and in adjusting the controls in place.
- Undertaking Data Protection Impact Assessments and System Security Level risk assessments as methods through which information assets can be risk assessed and assured they comply with the required standards.

## 5. Implementation

5.1 This policy will be available to all staff for use in relation to the specific function of the policy.

5.2 All managers are responsible for ensuring that relevant staff within the CCG have read and understood this document and are competent to carry out their duties in accordance with the procedures described.

5.3 This policy will be implemented in the following ways:

- Mandatory Data Security Awareness training
- Regular communications to staff on new Information Governance policies and procedures Guidance and access to policies and procedures
- The Information Governance Team will be the key contact point for staff support within the organisation
- Regular audit of information governance processes undertaken in line with information governance policy and procedures in key areas i.e. records management, confidentiality, information security, freedom of information and data quality
- Monitoring of information governance processes through the Data Security & Protection Toolkit.

## 6. Training Implications

The Executive Committee has ultimate responsibility for ensuring that the necessary training or education needs and methods required to implement the policy or procedure(s) are identified and resourced or built into the delivery planning process. This may include identification of external training providers or development of an internal training process.

## 7. Related Documents

7.1 Legislation and statutory requirements

- Cabinet Office (1990) *Computer Misuse Act 1990*. London. HMSO
- Cabinet Office (2018) *Data Protection Act 2018* London. HMSO.
- Cabinet Office (1990) *Access to Health Records Act 1990.*London. HMSO.
- Cabinet Office (2000) *Freedom of Information Act 2000*. London. HMSO.
- Cabinet Office (2004) *Environmental Information Regulations 2004*. London. HMSO.
- Cabinet Office (2006) *Fraud Act 2006*. London. HMSO
- EU General Data Protection Regulations 2016

7.2 Best practice recommendations

- Department of Health's Records Management Code of Practice for Health & Social Care 2016
- NHS Confidentiality Code of Practice
- Common Law Duty of Confidentiality

## 8. Monitoring, Review and Archiving

8.1 Monitoring

8.1.1 The Governing Body will agree a method for monitoring the dissemination and implementation of this policy. Monitoring information will be recorded in the policy database.

8.1.2 All staff must adhere to this policy and comply with applicable UK legislation and any regulatory requirements for information governance.

8.1.3 Failure to follow this policy and related information governance policy and procedures may lead to disciplinary, criminal or civil action being taken against the staff member.

8.1.4 Different methods will be used for monitoring different aspects of information governance including:

- Monitoring of information governance processes through the Data Security and Protection Toolkit.
- Audit of information flows to ensure confidential information is being transferred securely and in order to minimise information risk.
- Regular audit of information governance processes undertaken in line with information governance policy and procedures in key areas i.e. records management, confidentiality, information security, freedom of information, data quality.
- Action plans resulting from data protection impact assessments and system level security assessments are appropriately implemented to minimise information risk.

The organisation will, in conjunction with the internal and external audit, identify any areas for improvement of IG and information risk and development and agree appropriate action plans.

8.2 Review

8.2.1 The Governing Body 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.

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

8.2.3 For ease of reference for reviewers or approval bodies, changes should be noted in the ‘document history’ table on the second page of this document.

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

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

8.3 Archiving

The Governing Body will ensure that archived copies of superseded policy documents are retained in accordance with the Department of Health's Records Management Code of Practice for Health and Social Care 2016.

## 9. Equality Analysis

### 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<br>Role: Senior Governance Manager, IG & DPO |

### Title of the service/project or policy:

| |
|---|
| Information Governance and Information Risk Policy |

| |
|---|
| Is this a:<br>St. Strategy / Policy ☐ Service Review ☐ Project<br>If other, please specify: |

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

| |
|---|
| This policy sets out the CCG's commitment to the confidentiality of personal information and its responsibilities with regard to the disclosure of such information. |

| Questions | Yes | No |
|---|---|---|
| Could there be an existing or potential impact on any of the protected characteristic groups? | | X |

It aims to ensure all staff whether directly employed or contracted are aware of their responsibilities towards the confidentiality of personal information.

**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:

| | | |
|---|---|---|
| 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:<br>• Eliminating unlawful discrimination, victimisation and harassment<br>• Advancing equality of opportunity<br>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 Sunderland CCGs' Information Governance and Information Risk 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 | August 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.

## Appendix A

# Duties and Responsibilities

| | |
|---|---|
| **Executive Committee** | The Governing Body has delegated responsibility to the Executive Committee 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. |
| **Deputy Chief Officer** | The Deputy Chief Officer has overall responsibility for the strategic direction and operational management, including ensuring that CCG process documents comply with all legal, statutory and good practice guidance requirements.<br><br>The Deputy Chief Officer has overall responsibility for ensuring that information risks are assessed and mitigated to an acceptable level and handled in a similar manner to other major risks such as financial.<br><br>The Deputy Chief Officer will identify additional resources where necessary to support the IG agenda. |
| **Executive Committee (responsible for IG)** | The Executive Committee has a responsibility to:<br>• Develop the Information Governance agenda across the organisation.<br>• Monitor the organisation's progress in this area using the NHS Digital Data Security & Protection Toolkit.<br>• Ensure action plans are developed in each of the different areas of IG to meet the IG standards and requirements.<br>• Carry out specific pieces of work in accordance with the action plans.<br>• Ensure IG Policies and procedures are developed, implemented and reviewed appropriately.<br>• Ensure all risks and incidents associated with IG and Information Risk are identified, logged, actioned and monitored routinely. |
| **Information Governance Team (CSU)** | The Information Governance Team has a responsibility to:<br>• Provide information governance support to staff in the organisation.<br>• Co-ordinate different areas of information governance and ensure progress against key standards and requirements.<br>• In collaboration with IT, develop, implement and monitor information security across the organisation.<br>• To support the CCG in evidence collation, upload and publication of the Data Security & Protection Toolkit. |

| | |
|---|---|
| **Freedom of Information (FOI) Lead(CSU)** | Freedom of Information(FOI) Lead (CSU); has a responsibility to:<br>• Appropriate policies and procedures relating to FOI are developed and available to staff.<br>• Ensure the "Guide to Information" (formerly Publication Scheme) is kept up to date and available on the public website.<br>• Ensure all FOI requests and exemptions are processed in an appropriately, timely manner.<br>• Investigations are dealt with appropriately. |
| **CSU Staff** | Whilst working on behalf of the CCG, CSU staff will be expected to comply with all policies, procedures and expected standards of behaviour within the CCG, however they will continue to be governed by all policies and procedures. |
| **Caldicott Guardian** | The Caldicott Guardian has a responsibility to:<br>• Ensure the organisation satisfies the highest confidentiality standards.<br>• Advise on lawful and ethical processing of information.<br>• Ensure appropriate processes and procedures are established to enable the organisation to act in accordance with the Caldicott principles.<br>• Represent and champion information governance and report issues at Governing Body/Senior Management Team level.<br>• Take a key role in ensuring standards of confidentiality in relation to the National Programme for IT.<br>• Act as signatory for high level information sharing agreements. |
| **Senior Information Risk Owner (SIRO)** | The Senior Information Risk Owner (SIRO) has a responsibility to:<br>• Oversee the development of an Information Governance & Information Risk Policy and Strategy and its implementation.<br>• Take ownership of risk assessment process for information risk.<br>• Review and agree action in respect of identified information risks.<br>• Ensure that the Organisation approach to information risk is effective in terms of resource, commitment and execution and that this is communicated to all staff.<br>• Provide a focal point for the resolution and/or discussion of information risk issues.<br>• Ensure the Governing Body is adequately briefed on information risk issues.<br>• Successfully complete strategic information risk management training at least annually. |

| | |
|---|---|
| **Information Asset Owners** | Information Asset Owners (IAOs) are responsible for:<br>• Liaising with records management/IG leads to ensure that records management practices are in line with the guidance and protocols on confidentiality.<br>• Ensuring appropriate record audits are undertaken.<br>• Ensuring appropriate information governance /confidentiality clauses are in third party contracts relating to records management such as secondary storage, scanning companies before using the company.<br>• Ensuring appropriate consideration is given to records management within business continuity plans.<br>• Ensuring they obtain appropriate certifications of destruction.<br>• Investigate and take relevant action on any potential breaches of this policy supported by other applicable staff in line with existing procedures. |
| **Information Asset Administrators (IAA)** | Information Asset Administrators (IAA) support the IAO to ensure that policies and procedures are followed, recognise actual and potential security incidents, consult the appropriate IAO on incident management, and ensure that information asset registers are accurate and up to date. |
| **Line Managers** | Line managers have a responsibility to:<br>• Ensure all current, new and temporary staff are instructed in their responsibilities in relation to the Information Governance and Information Risk Policy & Strategy and related policies and procedures, and work in a manner consistent with this policy.<br>• Ensure staff are appropriately trained in information governance in line with the requirements of their post.<br>• In certain circumstances, to support equality & diversity, line managers will need to consider individual requirements of staff to support good practice in complying with this policy.<br>• Investigate and take relevant action on any potential breaches of this policy supported by risk management leads and IG Team in line with existing procedures. |