NHS

Coventry and Rugby
Clinical Commissioning Group

INFORMATION RISK POLICY

Accountable Director:	Chief Operating Officer
Policy Author:	Arden & GEM CSU
Approved by:	Coventry and Rugby Clinical Commissioning Group Governing Body
Date approved:	13 January 2016
Issue date:	14 January 2016
Review date:	November 2018
Person responsible for instigation:	Head of Corporate Affairs
Links to Standards – Care Quality Commission and NHSLA	CQC - Outcome 21 NHSLA - Standard 1, Criterion 8
Implementation plan in place:	
Equality Impact Assessment (EIA):	Yes

Source: Commissioning □
Corporate x
Community □

HR □
Estates □
Public Health □

Version control

V1.1	Prepared for authorisation April 2013
V1.2	Reviewed November 2015

Contents

1. Introduction

1.1 This policy document sets out NHS Coventry and Rugby CCG's Information Risk Policy.

1.2 NHS Coventry and Rugby CCG's Governing Body has approved the introduction and embedding of information risk management into the key controls and approval processes of all major business processes and functions of NHS Coventry and Rugby CCG. This decision reflects the high level of importance placed upon minimising information risk and safeguarding the interests of patients, staff and NHS Coventry and Rugby CCG itself.

1.3 Information risk is inherent in all administrative, clinical and business activities and everyone working for or on behalf of NHS Coventry and Rugby CCG continuously manages information risk. The Board recognises that the aim of information risk management is not to eliminate risk, but rather to provide the structural means to identify, prioritise and manage the risks involved in all NHS Coventry and Rugby CCG activities. It requires a balance between the cost of managing and treating information risks with the anticipated benefits that will be derived.

1.4 The Board acknowledges that information risk management is an essential element of broader information governance and is an integral part of good management practice. The intent is to embed information risk management in a very practical way into business processes and functions. This is achieved through key approval and review processes / controls – and not to impose risk management as an extra requirement.

1.5 It should be noted that this policy complements NHS Coventry and Rugby CCG's Risk Management Strategy, and does not supersede this relevant documentation.

2. Policy objectives

The Information Risk Policy has been created to:

- Protect NHS Coventry and Rugby CCG, its staff and its patients from information risks where the likelihood of occurrence and the consequences are significant;
- Provide a consistent risk management framework in which information risks will be identified, considered and addressed in key approval, review and control processes;
- Encourage pro-active rather than re-active risk management;
- Provide assistance to and improve the quality of decision making throughout NHS Coventry and Rugby CCG;
- Meet legal or statutory requirements; and
- Assist in safeguarding NHS Coventry and Rugby CCG's information assets.

The purpose of this policy is to formally establish NHS Coventry and Rugby CCG's position regarding its information risk management process. The intent is to embed information risk management in a very practical way into business processes and functions via key approval processes, review processes and controls, and not to impose information risk management as an extra requirement.

3. Policy statements

3.1 NHS Coventry and Rugby CCG's Senior Information Risk Owner (SIRO) is responsible for coordinating the development and maintenance of information risk management policies, procedures and standards for NHS Coventry and Rugby CCG.

3.2 The SIRO is responsible for the ongoing development and day-to-day management of NHS Coventry and Rugby CCG's Risk Management Programme for information privacy and security.

3.4 NHS Coventry and Rugby CCG Information Asset Owners (IAOs) shall ensure that information risk assessments are performed at least annually on all information assets where they have been assigned 'ownership', following guidance from the SIRO on assessment method, format, content, and frequency. IAOs shall submit the risk assessment results and associated mitigation plans to the SIRO for review, along with details of any assumptions or external dependencies. Mitigation plans shall include specific actions with expected completion dates, as well as an account of residual risks.

3.5 The SIRO shall advise the Accountable Officer and the Governing Body on information risk management strategies and provide periodic reports and briefings on Program progress.

3.6 NHS Coventry and Rugby CCG will undertake an annual information flow mapping exercise and from this exercise determine the information risks regarding its data flows within the organisation and/or with its delivery partners.

3.7 The reporting of information (including Information Security) risks and
incidents will be in line with NHS Coventry and Rugby CCG's overall risk management and incident reporting processes

3.8 NHS Coventry and Rugby CCG recognises that the outcome of information risk management approach may not eliminate information risk totally, but rather provide the organisation with the means to identify, prioritise and manage the risks and provide a balance between the cost of managing and treating risks, and the anticipated benefits that will be derived.

4. Policy scope

This policy is applicable to all departments and functions of NHS Coventry and Rugby CCG and adherence should be included in all contracts for outsourced or shared services. There are no exclusions.

5. Communication

This policy is to be made available to all NHS Coventry and Rugby CCG staff and observed by all members of staff, both clinical and administrative.

There will be an ongoing professional development and educational strategy to accompany the implementation of this policy.

6. Definitions

Key definitions are:

- **Risk**
  The chance of something happening, which will have an impact upon objectives. It is measured in terms of *consequence* and *likelihood*.
- **Consequence**
  The outcome of an event or situation, expressed qualitatively or quantitatively, being a loss, injury, disadvantage or gain. There may be a range of possible outcomes associated with an event.
- **Likelihood**
  A qualitative description or synonym for probability or frequency.
- **Risk Assessment**
  The overall process of risk analysis and risk evaluation.
- **Risk Management**
  The culture, processes and structures that are directed towards the effective management of potential opportunities and adverse effects.
- **Risk Treatment**
  Selection and implementation of appropriate options for dealing with risk. Conceptually, treatment options will involve one or a combination of the following five strategies:
    - Avoid the risk
    - Reduce the likelihood of occurrence
    - Reduce the consequences of occurrence
    - Transfer the risk
    - Retain/accept the risk
- **Risk Management Process**
  The systematic application of management policies, procedures and practices to the tasks of establishing the context, identifying, analysing, evaluating, treating, monitoring and communicating risk.

7. Responsibilities and contacts

7.1 Senior Information Risk Owner (SIRO)

- To delegate responsibilities to appropriate Information Asset Owners/Administrators within their organisational unit.
- To oversee the development of an Information Risk Policy, and a Strategy for implementing the policy within the existing Information Governance Framework.
- To take ownership of the risk assessment process for information risk, including review of the annual information risk assessment to support and inform the Annual Governance Statement.
- To review and agree action in respect of identified information risks.
- To ensure that the NHS Coventry and Rugby CCG's approach to information risk is effective in terms of resource, commitment and execution and that this is communicated to all staff.
- To provide a focal point for the resolution and/or discussion of information risk issues within their organisational unit.

7.2 SIRO Support Infrastructure

The following roles will form the supporting infrastructure for the SIRO in matters of information risk across NHS Coventry and Rugby CCG:

- Caldicott Guardian
- Arden & GEM CSU Information Governance Consultant

7.3 Information Asset Owners/Administrators

Information Asset Owners (IAOs) are accountable to the SIRO and will provide assurance that information risk is being identified and managed effectively for those information assets that they have been assigned ownership of. Information Asset Administrators (IAAs) will usually be staff who have day-to-day responsibility for management of information risks affecting one or more assets, and report these to the IAOs.

7.4 Managers

Managers are responsible for ensuring that this policy and supporting standards and guidelines, including NHS Coventry and Rugby CCG's Confidentiality Code of Conduct, are built into local processes and that there is ongoing compliance.

7.5 Commissioners

NHS Coventry and Rugby CCG's Commissioning staff are additionally responsible for ensuring that all Information Governance arrangements are in place and monitored in all organisations contracted to provide services to

NHS Coventry and Rugby CCG, either under a full contract or through service level agreements

7.6 All Staff

All members of staff have a responsibility to ensure the effectiveness of risk management within NHS Coventry and Rugby CCG. Please see the Risk Management Strategy for further details.

8 . Monitoring and Review

This policy will be reviewed once a year by the Information Governance Steering Group.

Auditing of this document should be done at least every two years based on monitoring the effectiveness of the policy in line with legislation and guidelines.

9. Related policies/guidelines

Information Governance Strategy

Serious & Untoward Incident Policy

Risk Management Strategy

Information Security Policy

Safe Haven Policy

Records Management Strategy and Policy

Data Encryption Policy

Other Relevant Documentation:
Information Asset Register
Data protection Act 1998
Human Rights Act 1998
Computer Misuse Act 1990

10.0 Equality and Impact Assessment

Department	**Corporate Affairs**	Name of person completing EIA	**Mandy Smith**
Date of EIA	**November 2015**	Accountable CCG Lead	**Rebecca Blyth**
		CCG Sign off and date	

Piece of work being assessed	**Information Risk Policy**
Aims of this piece of work	**To set out and promote a culture of good practice around Information Risk Management within the CCG**
Other partners/stakeholders involved	**Information Governance Steering Group members and consultation respondents**
Who will be affected by this piece of work?	**All CCG staff, Governing Body members, third party contractors**

Single Equality Scheme Strand	**Baseline data and research on the population that this piece of work will affect.** What is available? E.g. population data, service user data. What does it show? Are there any gaps? Use both quantitative data and qualitative data where possible. **Include consultation with service users wherever possible**	**Is there likely to be a differential impact?** Yes, no, unknown.
Gender	There is no identifiable data that suggests that females, males or transgender people would be affected by this policy	No
Race	Compliance with the policy should be undertaken by all people. Different ethnicities should not be impacted upon, someone's race should not impact their ability to comply with this policy	No
Disability	The identified risk surrounding people with a learning/sensory/motor disability being able to access the policy and its content	Yes
Religion/ belief	There is no data to suggest that someone's religious beliefs would be impacted upon by this policy	No

Sexual orientation	There is no data to suggest that someone’s sexual orientation would be impacted upon by this policy	No
Age	There is no data to suggest that someone’s age would be impacted upon by this policy.	No
Social deprivation	There is no data to suggest that someone’s social deprivation status would be impacted upon by this policy	No
Carers	Someone’s status as a carer would not be impacted upon by this policy	No
Human rights	Will this piece of work affect anyone’s human rights?	No

Equality Impact Assessment Action Plan

			← **CCG** →		
Strand	**Issue**	**Suggested action(s)**	**How will you measure the outcome/impact**	**Timescale**	**Lead**
Disability	Accessing the policy and its content	The document will be made available in alternative formats if required. This provision is set out in the framework	Annually measure the number of requests and ability to accommodate	Annually	