INFORMATION RISK POLICY

Document History

Document Reference:	IG10
Version:	Revised Policy
Ratified by:	SL/SWL CCG Senior Leadership Teams
Date ratified	March 2018
Name of originator/author	Information Governance Services
Name of responsible committee/individual:	Senior Leadership Team
Date issued:	March 2018
Review Date:	February 2021
Target audience:	All Staff within the CCG whether operating directly or providing services to other organisations under a service level agreement or joint agreement and to none executive directors, contracted third parties (including agency staff), locums, students, volunteers, trainees, visiting professionals or researchers, secondees and other staff on temporary placements within the organisation.
Distributed via:	Website
Document Purpose:	This document sets out the procedure to ensure that all information assets are identified and regularly assessed to ensure the confidentiality and security of the organisations' information is maintained.

South Lincolnshire CCG
South West Lincolnshire CCG

Version control sheet

Version	Section/Para/Appendix	Version/Description of Amendments	Date	Author	Version
Revised Version serving SL and SWL CCGs (dual branding)	Policy Review	Incorporates specific reference to impending General Data Protection Regulation (Revised as a dual branded policy for NHS South Lincolnshire CCG and NHS South West Lincolnshire CCG) Replaces existing policies within SLCCG and SWLCCG referenced IG10.	26/02/2018	JE	1

ASSISTANCE WITH THE APPLICATION OF THIS POLICY AND UPDATES

This policy has been prepared so as to reflect the law as at 14 February 2018. The policy will require periodic review to reflect subsequent changes to the law. Under the General Data Protection Regulation (GDPR) (which will apply from 28th May 2018), personal data must be processed in accordance with certain principles. While these are broadly similar to those under the Data Protection Directive (DPD), the wording has changed and they all centre on the concept of accountability.

The GDPR applies to 'controllers' and 'processors'; A controller determines the purposes and means of processing personal data whilst a processor is responsible for processing personal data on behalf of a controller. If you are a processor, the GDPR places specific legal obligations on you; for example, you are required to maintain records of personal data and processing activities. You will have legal liability if you are responsible for a breach. However, if you are a controller, you are not relieved of your obligations where a processor is involved – the GDPR places further obligations on you to ensure your contracts with processors comply with the GDPR. The General Data Protection Regulations (GDPR) (Regulation (EU) 2016/679) – is a regulation by which the European Parliament, the Council of the European Union and the European Commission intend to strengthen and unify data protection for all individuals within the European Union. GDPR applies to those who have a day to day responsibility for data protection. This should be read in conjunction with the CCGs' Information Governance Staff Handbook and the Privacy Impact Assessment Policy.

Contents

1.0 Introduction

1.1 Clinical Commissioning Groups (CCGs) accepted responsibility on 01/04/2013 for functions that Primary Care Trusts (PCTs) previously undertook i.e. planning, designing and managing local health provision.

1.2 In order to achieve this, the CCG will work with patients and health and social care partners e.g. local hospitals, local authorities, local community groups etc. to ensure that services meet local needs within their designated geographical boundaries. Risks must be effectively managed and previous lessons that have been learnt from risk associated mistakes must be adequately cascaded to ensure that the CCG does not repeat them.

1.3 All staff should be mindful that risk management responsibilities are not the sole responsibility of I.T. or Information Governance staff. All employees have an important role to play in order to ensure that risks are minimised and when encountered appropriately managed. It is important to remember that risk management is not about apportioning blame, but about promoting a fair and responsible culture, which contributes to learning and improvements when mistakes may occur, but that the consequences of failure to manage information risks adequately can be both corporate and individual. This policy contains details about the organisational responsibilities to manage risks and the processes that are used.

2. Purpose & Scope

2.1 In order to ensure that information held by CCGs is at a minimum risk of being compromised, CCGs will need to continue to build upon the strong foundations previously embedded by PCTs with regard to implementing effective, overarching, Information Governance Frameworks and risk management.

2.2 The Information Risk Policy has been created to:

- Protect the CCG, its staff (and board members) 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 fully considered and addressed during key approval, review and control processes
- Encourage a pro-active approach to managing risks, rather than a re-active risk management method
- Provide structure, transparency and assistance to improve the quality of decision making throughout the organisation
- Meet all legal or statutory requirements
- Assist in adequately safeguarding the CCG's information assets

2.3 This policy is applicable to all areas of the CCG and its staff inclusive of contractors and staff that may be provided through external agencies. The necessity of full adherence will be detailed and included within all contracts and for outsourced or

shared services.

2.4 The CCG 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 the CCG. This decision reflects the high level of importance placed upon minimising information risk and safeguarding the interests of patients, staff and the CCG itself.

2.5 Information risk is inherent in all administrative and business activities and everyone working for or on behalf of the CCG must effectively manage information risks for which they are responsible. The Governing Body recognises that the aim of information risk management is not to eliminate risk, but rather to provide a structured approach to accurately identify, prioritise and manage the risks involved in all CCG related activities. It requires a balance between the cost of managing and treating information risks with the anticipated benefits that will be derived.

2.6 The CCG acknowledges that information risk management is an essential element of broader Information Governance (IG) and is an integral part of good management practice. The intent is to embed information risk management in a practical and achievable way into business processes and functions, so that there is a clear, structured process that staff can easily follow. This is achieved through key approval and the frequent review of processes and controls. Risk management should not be considered as a burdensome extra requirement for the organisation to undertake, but effectively integrated as a matter of routine in working towards achieving best practice management standards.

3. Policy Objectives

3.1 The principal objectives of the Risk Management function are:

- To assist with the identification of all reasonably foreseeable risks, particularly which may have potentially adverse effects on the quality of care, confidentiality of patient information, safety of patients, staff and visitors (Risk Identification)
- To assist and support in the assessment of risks in terms of likelihood and severity (Risk Assessment)
- To ensure risk ratings are applied to identified risks (Risk Quantification)
- To identify the appropriate level of management to be responsible for the risk (Risk Owner)
- To take positive action to eliminate or reduce risks to as low as is reasonably practicable and continually review these actions (Risk Treatment)
- To keep the IG Steering Group (or equivalent) Board and Senior Management appraised of the significant risks present across the CCG (principally via the Risk Register and Risk reports)
- To create an escalation and accountability framework to help ensure satisfactory risk mitigation processes and Risk Owners are encouraged and supported in their task.

4. Key Responsibilities

4.1 The Chief Officer/Accountable Officer of the organisation has overall accountability and responsibility for Information Governance within the organisation and will provide assurance, through the Annual Governance Statement, that all risks to the organisation, including those relating to information, are effectively managed and mitigated.

4.2 The CCG Senior Information Risk Owner (SIRO) is responsible for coordinating the development and maintenance of all information risk management policies, procedures and standards for the CCG.

4.3 The SIRO will act as an advocate for information risk on the CCG Board and during internal discussions and will provide written advice to the Accountable Officer on the content of the annual Governance Statement (SIC) in regard to information risk.

4.4 The SIRO is responsible for the 'on-going' development and day-to-day management of the CCG's Risk Management Programme for information privacy and security.

4.5 Summary of SIRO key responsibilities are to:

- Oversee the development of an Information Risk Policy and a Strategy for implementing the policy within the existing information governance framework
- Take ownership of the risk assessment process for information risk, including review of an annual information risk assessment to support and inform the Annual Governance Statement
- Review and agree action in respect of identified information risks
- Ensure that the organisation's approach to information risk is effective in terms of resource, commitment and execution and that this is communicated to all staff, including the board
- Provide a focal point for the resolution and/or discussion of information risk issues
- Ensure the Board is adequately briefed on information risk issues

4.6 CCG Information Asset Owners (IAOs) shall ensure that:

- Information risk assessments are performed annually (at least) or as required
- They undertake and submit risk assessments for review using standard guidance and methodologies that have been endorsed and approved by the CCG

5. Information Asset Registers

5.1 The CCG will establish a programme to ensure that their Information Assets (IAs) are identified and assigned to an Information Asset Owner. The SIRO will oversee a review of the organisation's asset register to ensure it is kept up to

date, complete and robust. All critical IAs will be identified and included within the Information Asset Register (IAR), together with details of business criticality, the IAO, the Information Asset Administrator (IAA) and risk reviews to be carried out.

5.2 In order to improve the usability and maintainability, the Information Asset register may be organised by service, rather than by location.

6. Communication

6.1 This policy will be made available to all employees of the CCG and observed by all members of staff, clinical and administrative, both temporary and permanent.

7. Training

7.1 All users will be trained in the use of systems and procedures to ensure that quality and appropriate handling of information, in order to minimise risks to the organisation from poor information governance.

7.2 All key roles (SIRO, Caldicott Guardian), IAOs will undertake information risk management training at least annually, if training materials are available via NHS HSCIC/NHS Digital.

8. Equality & Diversity Impact Assessment

8.1 This document has been assessed for equality impact on the protected groups, as set out in the Equality Act 2010. This policy is applicable to every member of staff within the CCG irrespective of their age, disability, sex, gender reassignment, pregnancy, maternity, race (which includes colour, nationality and ethnic or national origins), sexual orientation, religion or belief, marital status or civil partnership.

9. Policy Review

9.1 This policy will be reviewed by the CSU's Information Governance Steering Group and the CCG's Quality & Governance Committee (or equivalent) annually. This may be subject to change and the policy may be reviewed in the event of serious untoward incidents or a change in national guidance.

10. Contacts

Caldicott Guardian	Elizabeth Ball (SLCCG) Pamela Palmer (SWLCCG)
Senior Information Risk Owner	Jo Wright
CCG IG Lead	Jen Rousseau
IG Support	OPTUM CSS Lynne.wray1@nhs.net jemptage@nhs.net

Appendix A - 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.

Annual Governance Statement (AGS): High quality and proportionate internal control systems will help organisations achieve their aims. The Annual Governance Statement (AGS) is a public accountability document that describes the effectiveness of internal controls in an organisation and is personally signed by the Chief Officer.

Appendix 1 - Equality Analysis Initial Assessment

Title of the change proposal or policy:

Information Risk Policy

Brief description of the proposal:

To ensure that the policy amends are fit for purpose, that the policy is legally compliant, complies with legislative requirements and includes details of the European Directive – General Data Protection Regulations.

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

June Emptage – Information Governance Officer

Date of assessment: 26th February 2018

Please answer the following questions in relation to the proposed change:

Will it affect employees, customers, and/or the public? Please state which.

Yes it will affect all employees and those who enter into contractual arrangements with the organisation.

Is it a major change affecting how a service or policy is delivered or accessed?

No – although it introduces new General Data Protection Regulations which will be mandatory in May 2018

Will it have an effect on how other organisations operate in terms of equality?

No

If you conclude that there will not be a detrimental impact on any equality group, caused by the proposed change, please state how you have reached that conclusion:

No anticipated detrimental impact on any equality group. The policy adheres to the legislative requirements which are applicable to all.