Northern, Eastern and Western Devon
Clinical Commissioning Group

Date		December 2014		
Policy title		Information Risk Management policy		
Author(s)		Clare Doble, Deputy Head of Governance and IG Lead John Harle, Governance Manager		
Supporting Executive(s)		Anne Forbes, Interim Director of Corporate Development & Compliance		
Purpose of Policy	✓	**Decision**		
		Assurance		
		Information		✓
FOI Status	✓	**Public**		✓
		Private		
Category of Policy	✓	**Decision**		
		Position Statement		
		Information		✓
Does this document place Individuals at the Centre		**Y**	**N**	Y
Actions Requested				
Which other committees has this item been to?		Governance Steering Group and Quality Committee		
Reference to other documents		Risk Strategy and Risk policy		
Have the legal implications been considered?				
Equality Impact Assessment				
Who does the proposed piece of work affect?		Staff ✓ Patients ✓ Carers ✓ Public ✓		
			Yes	No
1. Will the proposal have any impact on discrimination, equality				✓

of opportunity or relations between groups?		
2. Is the proposal controversial in any way (including media, academic, voluntary or sector specific interest) about the proposed work?		✓
3. Will there be a positive benefit to the users or workforce as a result of the proposed work?	✓	
4. Will the users or workforce be disadvantaged as a result of the proposed work?		✓
5. Is there doubt about answers to any of the above questions (e.g. there is not enough information to draw a conclusion)?		✓
If the answer to any of the above questions is yes (other than question 3) or you are unsure of your answers to any of the above you should provide further information using **Screening Form One** *available from Corporate Services*		
If an equality assessment is not required briefly explain why and provide evidence for the decision.		

NEW Devon CCG has made every effort to ensure this policy does not have the effect of discriminating, directly or indirectly, against employees, patients, contractors or visitors on grounds of race, colour, age, nationality, ethnic (or national) origin, sex, sexual orientation, marital status, religious belief or disability. This policy will apply equally to full and part time employees. All NEW Devon CCG policies can be provided in large print or Braille formats if requested, and language line interpreter services are available to individuals of different nationalities who require them.

Reference to Core Strategies and Corporate Objectives

Core Strategies, we will:	Corporate Objective	Does this report reference to the Core Strategies/ Corporate Objectives	
		✓	X
1. Take joint ownership with partners and the public for creating sustainable health and care services	1.1 Develop people, and those who support them, to value strengths and personal qualities in all that they do	✓	
	1.2 Listen to people and take action on what they say about services	✓	
2. Implement systems that make the best use of valuable health resources, every time	2.1 Innovate to increase productivity and reduce waste	✓	
	2.2 Commission safe services and reduce avoidable harm	✓	

3. Commission to prevent ill health, promote wellbeing and help people with long-term conditions to live well	3.1 Support people to make healthy lifestyle choices and understand the care, treatment and services available to them	✓
	3.2 Commission services with partners to reduce health inequalities and improve people's lives	✓

Northern, Eastern and Western Devon
Clinical Commissioning Group

Document Status:	Ratified
Version:	V 1.3

DOCUMENT CHANGE HISTORY		
Version:	**Date:**	**Comments (i.e. viewed, or reviewed, amended , approved by person or committee)**
V0.1	29/05/2013	Initial draft
V0.2	20/06/2013	Incorporated SIRO comments
V1	17/07/2013	Updated
V1.1	October 2014	Amended due to staffing changes
V1.2	December 2014	Ratified at Governing Body
V1.3	October 2017	Updated to reflect title changes
Authors:	John Harle Governance Manager	
Scrutinised by: (name & title) **Date:**	Clare Doble, Deputy Head of Governance and IG Lead	
Document Reference:	IG Toolkit – Information Security Assurance	
Review date of approved document:	October 2018	

CONTENTS

Linked strategies, policies and other documents	IG Toolkit – Information Security Assurance SIRI Policy Risk Strategy and Risk policy

1. Introduction

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

1.2 Information risk is inherent in all administrative and business activities and everyone working for, or on behalf of the organisations continuously manages information risk. The governing body 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 of the organisation's activities. It requires a balance between the cost of managing and treating information risks with the anticipated benefits that will be derived.

1.3 The Governing Body 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.

2. Purpose

2.1 The Information Risk Management policy has been created to:

- Protect patients, the organisation and its staff 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 proactive rather than reactive risk management;
- Provide assistance to and improve the quality of decision making throughout the organisation;
- Meet legal and/or statutory requirements; and
- Assist in the safeguarding of the organisation's information assets.

3. Policy statements

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

3.2 The SIRO is responsible for the ongoing development and day to day management of the organisations Risk Management program for privacy and security.

3.3 Information Asset Owners (IAO) are senior individuals involved in running the relevant business areas. Their role is to understand and address risks to the information assets they 'own' and to provide assurance to the SIRO on the security and use of those assets.

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

3.5 These Information Asset Owners (IAO's) are likely to be supported by Information Asset Administrators (IAAs), or equivalents e.g. User Administrators, who are operational staff with day to day responsibility for managing risks to their information assets.

3.6 Identified information risks will be managed in line with the organisations Risk Management Strategy and use the organisations Risk Management policy mechanisms.

3.7 The SIRO shall advise the Chief Officer and the organisations Governing Body on information risk management strategies and provide periodic reports and briefings on program progress.

3.8 The organisation will implement the NHS Information Risk Management Good Practice Guide.

4. Policy scope

4.1 This policy is applicable to all areas of the organisation and adherence should be included in all contracts for outsources or shared services. There are no exclusions.

5. Communication

5.1 This policy is to be made available to all organisational staff and observed by all members of staff, both clinical and administrative.

5.2 There will be an on-going professional development and educational strategy to accompany the implementation of this policy.

6. Related Information

6.1 This Information Security Management System (ISMS) is the organisations major mechanism for the management of information security risk and will be the vehicle through which the NHS Information Risk Management and Good Practice Guide will be implemented.

6.2 Information risks arising from IT projects are managed as part of the management process.

6.3 Analysis of the outstanding and residual information security risks will be used to identify those for entering in the organisation's Corporate Risk Register.

7. Definitions

7.1 The key definitions are:

- **Risk** – the chance of something occurring that 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 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; and
    - 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.

Information Security Management System (ISMS) – Is a set of frameworks that contain policies and procedures for tackling security risks in an organization. The focus of an ISMS is to ensure business continuity by minimizing all security risks to information assets and limiting security breach impacts to a bare minimum.

8. Responsibilities and contacts

8.1 Nick Roberts – Accountable Officer.
8.2 SIRO – Hugh Groves, Chief Finance Officer
8.3 Caldicott – Lorna Collingwood-Burke
8.4 General Information Security Advice – Gary Kennington

9. Additional Resources

9.1 The NHS Information Risk Management "Good Practice Guide" provides guidance for those responsible for managing information risk within NHS organisations. It reflects Government guidelines and is consistent with the Cabinet Office report on 'Data Handling Procedures within Government'

9.2 The key requirement is for information risk to 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. Assurances need to be provided in a consistent manner. To achieve this, a structured approach is needed, building upon the existing information governance framework within which many parts of the NHS are already working. This structured approach relies upon the identification of information assets and assigning 'ownership' of assets to senior accountable staff.

9.3 This document can be found at:http://systems.hscic.gov.uk/infogov/security/risk/inforiskmgtgpg.pdf

9.4 The NHS Information Security Management, NHS Code of Practice can be located http://systems.hscic.gov.uk/infogov/codes/securitycode.pdf