NHS
North Hampshire
Clinical Commissioning Group

Information Risk Management Policy and Strategy

COR/018/v1.10

Subject and version number of document:	Information Risk Management Policy and Strategy v1.10
Unique Reference Number:	COR/18/v1.10
Operative date:	16 March 2015
Author:	NHS South Commissioning Support Unit
Review date:	28 February 2018
For action by:	All permanent and temporary / agency staff and contractors
Policy statement:	To establish relevant lines of responsibility and conduct for all members of the CCG regarding information risk management.
Responsibility for dissemination to new staff:	Head of Business Development
Training Implications:	All permanent and temporary / agency staff and contractors
Further details and additional copies available from:	http://www.northhampshireccg.com/info.aspx?p=5 or via NHCCG Business Development team
Equality Analysis Completed?	This document includes a section about Equality Analysis (previously called Equality Impact Assessment), the aim being to encourage and support policy developers to demonstrate 'due regard' to the Equality Act 2010. This will be achieved if all new policies are assessed for equality impact at an early stage, and records kept of the equality analysis process and any actions identified.

Consultation Process	NHCCG Integrated Governance Committee
Approved and Ratified by (date):	NHCCG Governing Body (25 February 2014)

Version	Date Issued	Details	Brief Summary of Change	Author
1.0	20/02/2014	Draft	New document	NHS South Commissioning Support Unit, Information Governance Team
2.0	13.03.2015	Draft	Review & Update	Shelley Brown Senor IG Manager

For more information on the status of this policy, please contact:	
NHS South Commissioning Support Unit	Information Governance Team
Approved by	
Approval Date	
Next Review Date	
Responsibility for Review	Information Governance Team
Contributors	
Audience	All CCG officers and staff (which includes temporary staff, contractors and seconded staff) and CCG members in their capacity as commissioners.

Contents

1. Definition

Information risk management is the process of understanding and responding to factors that may lead to a failure in the confidentiality, integrity or availability of an information system.

Information security risk is the potential or real harm that may be done to a system or process and its related information, whether this is intentional or accidental.

2. Introduction

Information is a vital asset in the provision of high quality care and business processes. It is integral to the governance, service planning and performance management of North Hampshire Clinical Commissioning Group (the CCG).

To help ensure the safety of information in the CCG it is essential that information risk management is embedded into all business processes and functions.

It is critical that information risk be managed in a robust way across all services and departments and should not be considered to be the sole responsibility of one department/service area. For this to be successful, the CCG needs to implement a structured approach to information risk, the basis of which can be found in the existing information governance framework. Empirical to this success is the need to identify all information assets and assign ownership to senior accountable staff.

Information risk should not be considered in isolation but be seen as an intrinsic part of the CCG Risk and Safety Strategy.

3. Purpose

The purpose of this document is to establish relevant lines of responsibility and conduct for all members of the CCG staff regarding information risk management. This document applies to all employees of the CCG including permanent staff, contractors and temporary/agency staff.

As part of the CCG overarching information governance and risk management strategies it must ensure that:

- Information is protected against unauthorised access.
- Confidentiality of information is assured.
- Integrity of information is maintained.
- Regulatory requirements and legislation are met.

- IT systems are used in such a way as to prevent cyber-attacks or unauthorised disclosure, destruction or modification of information and the integrity of all systems are maintained.
- Strict access controls are applied to ensure that information, in whatever form, can only be accessed by those who are authorised to see it.
- Information security training is available to all staff via the Health and Social Care Information Centre (HSCIC) IG Training Tool website
- All breaches of information security whether actual or suspected, are investigated and reported by following the CCG incident reporting procedures

4. Accountability and Responsibilities

All information risks and incidents must be reported to the Head of Information Governance at NHS South Commissioning Unit.

Please see the CCG Information Incident Management and Reporting Procedures for further guidance on reporting incidents.

4.1 The Senior Information Risk Owner (SIRO)

The Senior Information Risk Owner (SIRO) has overall responsibility for ensuring that information risks are assessed and mitigated to an acceptable level.

The SIRO will act as advocate for information risk for the CCG. It is the SIROs responsibility to:

- Take ownership of the information risk assessment process
- Review and agree action in respect of identified information risk
- Ensure that the CCG approach to information risk is effective in terms of resource, commitment and execution and that it is communicated to all staff
- Provide a focal point for the resolution and/or discussion of information risk issues
- Ensure that Integrated Governance Committee (IGC) are adequately briefed on information risk issues
- Successfully complete strategic information risk management training on an annual basis

4.2 The Caldicott Guardian

The Caldicott Guardian will ensure that there are robust policies in place to ensure that patient information will remain confidential and seen only by those clinicians authorized to see the data. The Caldicott Guardian will ensure that breaches of this policy in respect of patient information are investigated and will also ensure that information Governance is duly regarded at Board level when appropriate**.**

4.3 NHS South Commissioning Support Unit Head of Information Governance (South CSU)

The Head of Information Governance for South Commissioning Support Unit (CSU) will, on behalf of the CCG SIRO and Caldicott Guardian liaise with the Information Security Manager to ensure that security risks to Personal Confidential Data (PcD) and business sensitive data are addressed.

The Information Security Manager for the CSU will ensure that assurance/s are provided to the CCG SIRO on the implementation of software countermeasures and management procedures in order protect CCG vital information/assets against the effects of malicious cyber software and other risks.

4.4 Information Asset Owners (IAO)

Information Asset Owners (IAOs) are senior members of staff responsible for providing assurance to the SIRO that information risks within their areas of responsibilities are identified, recorded and that controls are in place to mitigate those risks.

It is their responsibility to:

- Understand and address the risks to the information assets they own.
- Provide assurance to the SIRO on the security and use of those assets
- Ensure that all new projects (new systems and services) have a Privacy Impact Assessment (PIA) undertaken.
- Ensure that audits of Information Asset Register are completed annually for their department/service area.

4.5 Data Custodians

These are individuals who have responsibility for the day to day operation and administration of system/s they use.

It is their responsibility to:

- Ensure that all relevant policy and procedures are implemented and followed
- Have in place procedures to add or remove starters and leavers

NB: It is the line manager’s responsibility to ensure that a starters / leavers form is completed and that the IT Service desk are advised so that access to the network, files and email are enabled / disabled

- Recognise actual and potential security incidents

- Ensure that Information Registers are accurate and up to date. This should be done in conjunction with the CSU Information Governance Manager

4.6 Line Managers

Line Managers have a responsibility to:

- Ensure all current, new and temporary staff (including agency and contractors) receive appropriate training on their responsibilities for information risk and ensure that they read and understand all relevant CCG policies and procedures
- Investigate and take action on any potential breaches of the CCG policies and procedures, supported by the CSU Information Governance Manager

4.7 All Staff

All staff have a responsibility to:

- Adhere to all CCG risk and incident reporting procedures.
- Bring to their line manager’s attention any concerns regarding information governance and risk
- Report incidents in line with CCG Information Incident Management and Reporting Procedures

5. Information Risk Management Programme

The CCG information risk management programme has been aligned to the organisation’s business planning to support individual objectives and to ensure that they are adequately resourced.

The programme will cover:

- The balance between level of risk, tolerance of risk and the effort being used to manage the risk
- Identification of gaps between the current and target risk positions
- Progress being made against agreed information risk priorities
- The effectiveness of the risk management controls, including successes and failures

The following risk management audits will be carried out annually to identify, evaluate and mitigate any risk/weakness on the CCG information assets:

- Information Data Flow Mapping exercise
- Documented Information Asset Register

6. Risk Mitigation

Risk mitigation will:

- Be commensurate with the level of risk, it does not necessarily need to remove the risk
- Be kept simple to ensure manageability and must be communicated to all relevant staff
- Include monitoring and reporting on the level of information failures and breaches, so that the effectiveness of the controls can be assessed

Risks will be assessed in terms of general level of harm that could be reasonably caused if information were to be lost or compromised.

Mitigation should take the form of a wide range of controls directed at reducing the likelihood of an information security failure and reducing the amount of harm that failure could cause.

Controls covering both will reduce the likelihood of failure, reduce the amount of harm and will enhance overall mitigation.

Good practice controls will be identified and made easy for all staff to understand and apply. They will be supplemented with customised controls for specific higher risk circumstances.

A risk based approach means that there will always be some level of risk that will be tolerated. Controls will be applied under the constraints of:

- Expertise
- Cost
- Effort
- Practicability

These may be applied in phases or as an opportunity allows.

7. Legislation & Regulation

Relevant legislation and guidance:

- The Data Protection Act 1998
- Freedom of Information Act 2000
- Access to Health Records Act 1990
- Department of Health Records Management: NHS Code of Practice

- Common Law Duty of Confidentiality
- Information Security Management – SO/IEC 17799

Further guidance may be obtained from the Department of Health NHS Information Governance Guidance on Legal and Professional Obligations.

8. Related documents

- Information Governance Policy
- Information Incident Management and Reporting Procedures
- Confidentiality Audit Procedures
- Records Management Policy
- Safe Haven Policy

9. Monitoring and further mitigation of risk

The CCG needs to monitor for protection failures so they may deal with incidents and contain the harm they cause.

Analysis of incidents will support the CCG in understanding the real level of risk being experienced and in adjusting the controls in place.

The nature of information use and technology is constantly evolving and therefore requires regular re-evaluation of risk and controls to ensure that these do not constrain operational effectiveness or exceed risk tolerance levels.

10. Training, Distribution and Implementation of the Policy

10.1 Training

In order for this policy to be effective it is essential that all staff are aware of their obligations. This will be done by ensuring the following:

- All staff must complete their mandatory Induction Information Governance training by either attending a Face to Face training session (provided by the CSU IG Manager; or by completing the refresher training module on the Health and Social Care Information Centre (HSCIC) website within first week of employment. https://www.igtt.hscic.gov.uk/igte/index.cfmAs part of the CCGTraining Needs Analysis all staff undertaking information risk specialist roles e.g. SIRO, IAOs and Data Custodians should undertake additional training dependent upon their role, this should include relevant module on the HSCIC IG training tool https://www.igtt.hscic.gov.uk/igte/index.cfm

- Targeted and more general training for existing staff around information governance and information risk in particular.

10.2 Distribution

This policy will be available to all staff through the CCG intranet. It is the line manager's responsibility to ensure that staff are made aware of the existence of this policy and other information governance policies and guidance.

All staff will be notified of new or revised documents via staff updates.

10.3 Implementation of the Policy

This policy will be implemented in the following way:

- The policy will be posted on the CCG intranet and via the staff bulletin all staff will be made aware of the existence of this policy and other CCG policies.
- Senior staff including IAOs should ensure that appropriate arrangements are in place:
  - For the document to be cascaded to the appropriate staff
  - To identify any training requirements needed to achieve the required levels of knowledge for specific staff and roles i.e. Data Custodians
- All senior staff are responsible for ensuring that staff within their own departments/service areas have read and understood this document and are competent to carry out their duties in accordance with the procedures described.

11. Monitoring Compliance

All staff must adhere to this policy and comply with applicable UK legislation and regulatory requirements for information governance. Failure to follow this policy and relevant related policies and procedures may lead to disciplinary action being taken.

11.1 Methods to be used for monitoring compliance

- Monitoring of information security and risk processes through the relevant requirements in the Information Governance Toolkit
- Regular (no less than annual) audits of information flows to ensure that confidential information is being transferred securely in order to reduce information risk
- Implementation of action plans resulting from Information Governance Toolkit checklists, or internal or external auditor reports

12. Equality, diversity and mental capacity

The CCG recognises the diversity of the local community and those in its employment. The CCG aims to provide a safe environment free from discrimination and a place where all individuals are treated fairly, with dignity and appropriately to their need.

This policy was assessed against the NHS South CSU Impact Needs Requirement Assessment (INRA) tool to ensure that it does not introduce any unexpected or unwarranted equality and diversity disparities. The assessment confirmed that no amendments are required at this time.

This policy has been assessed and meets the requirements of the Mental Capacity Act 2005.

Appendix 1

North Hampshire CCG Equality Impact Analysis (EIA) Tool

Part 1 – Pre-Assessment Checklist

To determine if a **NEW** or **REVIEW** of a policy, procedure, strategy, service, proposal or function requires an Equality Impact Assessment:

		Yes/No
1.	Will the document have an impact on local people / staff? If '**Yes'**, go to question 2. If '**No**', then an Equality Impact Analysis is **not** required	**Yes**
2.	Are particular communities or groups likely to have different needs, experiences and / or attitudes in relation to the policy?	**No**
3.	Are there any aspects of the policy that could contribute to equality or inequality?	**No**
4.	Could the aims of the policy be in conflict with equal opportunity, elimination of discrimination, or promotion of good relations?	**No**

5. If this is an amendment to or a review of an existing policy, was the original impact assessed?

No

If the answer to any of the questions 2 – 5 is ‘**Yes’**, then complete:

Part 2 – *‘Rapid Assessment Checklist’* and High Level Action Plan

to decide if a Part 3 – *‘Full Equality Impact Assessment*’

NHS North Hampshire CCG Equality Impact Assessment Tool & Guidance v1 January 2015