Information Risk Policy

Author	Not Available
Responsible Director	Medical Director
Ratified By	Quality and Safety Committee
Ratified Date	December 2014
Review Date	December 2015
Version	1.1

Related Policies & Guidelines:

- Information Governance Policy
- Information Security Management Policy
- Records Management Policy

Contents

1. Introduction 3
2. Application: To Whom This Policy Applies 3
3. Policy Objectives 3
4. Policy Scope 4
5. Policy Principles 4
   5.1 Risk Appetite 4
   5.2 Strategic Information Risk Management Approach 4
   5.3 Risk of Harm Focus – Privacy 4
   5.4 Information Risk Processes 5
   5.5 Information Breach Management 5
   5.6 Escalation and Anonymous Reporting 5
   5.7 External Accountability and Progress Reporting 5
   5.8 Inspections, Reviews, Monitoring and Audit 6
6. Accountabilities and Responsibilities 6
7. Dissemination and Implementation 7
   7.1 Dissemination 7
   7.2 Implementation 7
8. Monitoring and Compliance 7
9. Non-Compliance 7

Appendix 1 – References 8

Amendment History

Version	Status	Date	Reason for Change	Authorised
1.1		December 2014	Review and formatting	Q&SC

1. Introduction

Central London Healthcare's (CLH) Quality and Safety sub-committee has approved the introduction and embedding of information risk management into the key controls and approval processes of all CLH's major business processes and functions. This decision reflects the high level of importance placed upon minimising information risk and safeguarding the interests of patients, staff, CLH and its practices.

CLH's Quality and Safety sub-committee accepts that information risk management is an essential element of broader information governance and is an integral part of good management practice. CLH aims to embed information risk management in a very practical way into all of its business processes and functions. This is achieved through key approval and review processes / controls – and not by imposing risk management as an extra requirement.

This policy specifically covers the risks associated with the handling of information. It sets out the framework for a formal information risk management programme in CLH by explicitly establishing responsibility for information risk management and its supervision, information risk processes and planning for information risk mitigation.

2. Application: To Whom This Policy Applies

This policy applies to all CLH staff, departments and functions that collect, transmit, retain or dispose of information in any form.

For the purpose of this policy, "staff" is used to refer to all staff regardless of occupation. This includes, but is not restricted to, permanent, fixed-term, contractors, agency, temporary, seconded, visiting, voluntary, and students.

This policy is also applicable to all third party data processors and emerging organisational forms that CLH in its capacity as a data controller has commissioned to deliver its services (data processors).

3. Policy Objectives

The purpose of this Information Risk Policy is to:

- Protect CLH and its staff
- 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 CLH's decision making
- Meet legal or statutory requirements
- Assist in safeguarding CLH's information assets

- Contribute towards CLH's compliance with requirements of the NHS Information Governance Toolkit

4. Policy Scope

This policy is applicable to all areas of CLH and adherence is included in all contracts for outsourced or shared services. There are no exclusions.

5. Policy Principles

5.1 Risk Appetite

CLH 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 CLH information activities. It requires ensuring a balance between the cost of managing and treating information risks vs. the anticipated benefits that will be derived from managing these risks.

CLH's risk appetite will therefore be informed by the cost effectiveness and proportionality of technological and human risk mitigating actions applied within a potential benefits vs. risk context to itself and relevant stakeholders.

CLH is not willing to accept information risks in most circumstances that may result in reputation damage, financial loss or exposure, major breakdown in information system or information integrity, significant incidents of regulatory non-compliance, potential risk of injury or harm to staff, patients, practices or any other relevant stakeholders.

5.2 Strategic Information Risk Management Approach

CLH will adopt an approach to information risk management which is consistent with guidance prepared by The National Archives with the support of the Cabinet Office; the UK Government's National Technical Authority for Information Assurance (CESG), Office of Cyber Security and Information Assurance (OCSIA), the Information Commissioner's Office (I CO) and the Ministry of Justice (MOJ).

5.3 Risk of Harm Focus – Privacy

CLH will be particularly careful to protect personal data, the release or loss of which could cause harm or distress to individuals.

CLH will identify and risk manage appropriately data it or its delivery partners hold whose release or loss could cause harm or distress to individuals. It will handle all such information as if it were at least "PROTECTED – PERSONAL DATA" while it is processed or stored within CLH or its partners, applying the measures in this policy. This will include as a minimum all data falling into one or both categories below.

- Any information that links one or more identifiable living person with information about them whose release would put them at significant risk of harm or distress
- Any source of information about 1000 or more identifiable individuals, other than information sourced from the public domain.

5.4 Information Risk Processes

Risk assessments will be performed for all CLH's information systems and critical information assets. Information Risk and or Privacy Impact Assessments will occur at the following times:

- At least six monthly
- Annually to inform the review of information risk by the SIRO to support the SIRO's written advice on the information risk content of the Statement of Internal Control to the Management Board
- At the inception of new systems, processes, applications, facilities, transition arrangements etc. that may impact the assurance of Information or Information Systems
- Before enhancements, upgrades, and conversions associated with critical systems, processes or applications and transition arrangements is implemented
- When NHS policy, regulation or legislation requires risk determination
- When the CLH Management Board or any other appropriate bodies requires it
- Annual data flow mapping exercises to determine the information risks regarding its data flows in transit

CLH will promote the conduct and publishing of Information Risk and or Privacy Impact Assessments as part of its information risk management programme.

5.5 Information Breach Management

Information incident reporting will be in accordance with CLH's incident breach management policy. A specific procedure for serious information incident breach management will be published and made available publicly.

5.6 Escalation and Anonymous Reporting

Staff who identify risks to CLH's information assets should alert the relevant IAO. If the IAO is not able to address the risk using the resources within their control, they should raise the matter with the SIRO, who if appropriate may escalate it further. All significant risks should be included in the IAOs assessment to the SIRO.

5.7 External Accountability and Progress Reporting

CLH will promote transparency about its information risks and incidents.

Each year CLH will set out in its Annual Report and Statement of Internal Control summary material on information risk, covering an overall judgement of the numbers of information risk incidents sufficiently significant for CLH's superior NHS bodies and/or the Information Commissioner to be informed.

5.8 Inspections, Reviews, Monitoring and Audit

The CLH Board, Quality and Safety sub-committee and other relevant committees will discuss information risk assessments regularly in order to manage existing risks and identify new ones.

There will be an annual assessment of information risk made by internal audit, which will support the SIRO in providing written assurance / advice to the CLH Board. The assessment will cover the effectiveness of the overarching policy. It will be informed by the written judgement of the SIRO, IAOs and the chair of the audit committee. In preparing for the annual assessment a number of assurance checks and inspections will be undertaken on information assets by internal audit.

6. Accountabilities and Responsibilities

The Head of Performance and Information will:

- Be the accountable officer for information risk

The Senior Information Risk Owner (SIRO) shall:

- Own the development and maintenance of information risk management policies, procedures and work programme
- Act as an advocate for information risk on the board and in internal discussions, and provide written advice to the Managing Director/CLH Board on the content of the Statement of Internal Control relating to information risk
- Be responsible for oversight and resourcing of the on-going development and day-to-day management of CLH's information risk management programme

IAOs shall:

- Ensure the confidentiality, integrity, and availability of all information that their system creates, receives, maintains, or transmits and protect against any reasonably anticipated threats or hazards to the security or integrity of such information
- Ensure that information risk assessments are performed at least once every six months on all information assets where they have been assigned ownership, following guidance from the SIRO on assessment method, format, content, and frequency
- 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
- Ensure all third parties and data processors involved in handling CLH's data, process personal data in accordance with the directions of the SIRO or his/her delegated representative or approved policy

Complementary support for the SIRO shall include persons and or bodies with the following responsibilities:

- CLH's Caldicott Guardian,
- CLH's Data Protection Officer
- CLH's Quality and Safety sub-committee

Staff will actively participate in identifying potential information risks in their area and contribute to the implementation of appropriate treatment actions.

7. Dissemination and Implementation

7.1 Dissemination

This policy is available on CLH's intranet and will be made available as part of the IG Management Framework on its public facing website. As with all new or updated polices, staff will be made aware of the policy via email.

7.2 Implementation

On-going Information Governance training and awareness raising sessions will continue at CLH to accompany the implementation of this policy.

8. Monitoring and Compliance

This will be through a various measures with regular reporting to senior management and committees. Example of monitoring actions will include for example the following:

- Internal Information Audits
- Review of contracts signed up to by CLH
- Number of staff trained
- Number of Privacy Impact Assessments
- Number of serious incidents
- Considerations of Information risk at senior management level committees

9. Non-Compliance

Failure to observe this policy may be regarded by CLH as gross misconduct. Disciplinary procedures, civil action or criminal proceedings may be instigated as a consequence of damage caused to an individual, CLH or its partner organisations by non-compliance with this policy.

Appendix 1 – References

- http://www.cabinetoffice.gov.uk/sites/default/files/resources/final-report.pdf
- http://www.nationalarchives.gov.uk/information-management/our-services/digital-continuity.htm
- http://www.cesg.gov.uk/products_services/iacs/iamm/media/iamm-assessment-framework.pdf
- http://www.connectingforhealth.nhs.uk/systemsandservices/infogov/security/risk/nhsinforiskmgt
- http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/privacy_impact_assessment_overview.pdf