NHS
Islington
Clinical Commissioning Group

GUIDANCE

1	**TITLE:**	**RISK ASSESSMENT AND MANAGEMENT**
2	**POLICY AREA:**	**INFORMATION GOVERNANCE**
3	**ACCOUNTABLE DIRECTOR FOR POLICY AREA:**	**DIRECTOR FOR QUALITY AND GOVERNANCE**
4	**GUIDANCE DRAFTED BY:**	**INTEGRATEDS GOVERNANCE MANAGER**
5	**SIGNED OFF BY**	**EXECUTIVE MANAGEMENT TEAM**
6	**RELATED DOCUMENTS:**	**[POLICIES] [OTHER DOCUMENTS]**

DOCUMENT CONTROL

Date	Version	Action	Amendments
17/3/14	2.1	Review and amendment of NCL information risk management policy	Put in CCG standard template, linked the CCG corporate risk management methodology and submitted for re-adoption

1. Introduction

Information risk is inherent in all the CCG's activities. The CCG recognises that the information risk must be managed and this guidance aims to provide the structural means to identify, prioritise and manage the risks to CCG activity. It is designed to help staff strike a balance between the cost of managing and treating information risks with the anticipated benefits that will be derived. The intent is to embed information risk management in a very practical way into business processes and functions.

Information risk management is an essential element of broader information governance and is an integral part of good management practice. This is achieved through key approval and review processes / controls – and not to impose risk management as an extra requirement.

2. Roles and Responsibilities

The Chief Officer has overall responsibility for ensuring that information risks are assessed and mitigated to an acceptable level. Information risks should be handled in a similar manner to other major risks such as financial, legal and reputational risks.

The Senior Information Risk Owner is responsible for the identification, scoping, definition and implementation of an information security risk programme. The Audit Committee will need to be aware of all information security risks and mitigation plans.

The lead for information governance will support staff identify and manage risks to information governance and information security.

Information Asset Owners look after information assets that are used to deliver the CCG's functions. 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.

All staff must ensure that policies and procedures are followed; that they recognise actual or potential security incidents; and that they consult colleagues in information governance on incident management, and keeping asset registers are accurate and up to date.

3. Security risks to information assets

There are a large number of sources of risk for information assets. Some of them are listed below but this list is not exhaustive and the relative balance of risks will depend on a number of factors e.g. are information assets shared with third parties.

Physical damage

- Natural events;
- technical failure;
- processing errors;

- software errors;
- equipment failure.

Loss

- This includes accidental loss and physical theft; and loss of access e.g. loss of essential services.

Malicious damage

- viruses;
- criminal activities;
- hackers;
- deliberate sharing of information by a member of staff.

Poor management of the information asset

- user errors and mis-operation;
- misuse of data, resources or services;
- unauthorised actions;
- compromise of information;
- personnel privilege abuse.

Governance

- changes or compromises to data classification or security policies;
- Particular risks around the handling of personally identifiable data.

When identified all risks should be considered and analysed.

4. Information security risk assessment and management method

a. Evaluating and Describing a Risk

A risk is something that might happen. It is made up of two components: likelihood (the chance that it will occur) and the consequence (what would the effect be if it did occur).

A typical risk approach is to rank each on a scale of one to five.

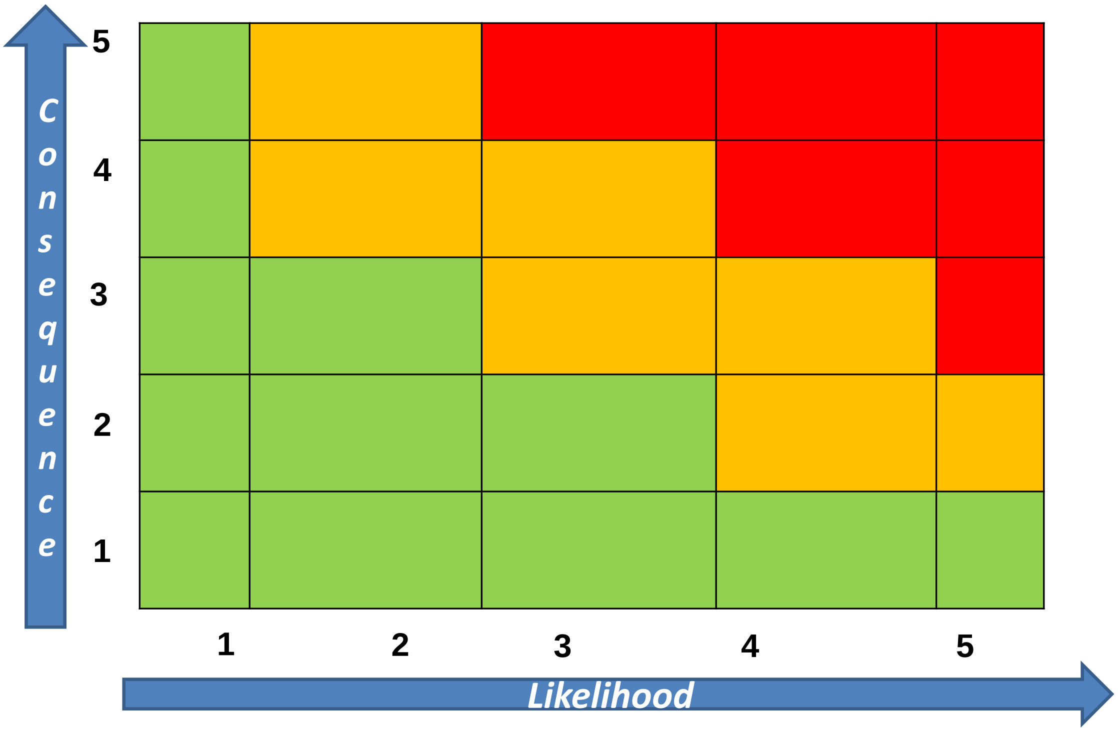
Scale	Likelihood	Impact
1	Rare	Minor
2	Unlikely	Moderate
3	Possible	Significant
4	Likely	Very significant
5	Almost Certain	Major

The CCG’s guidance on identifying and evaluating corporate risks describes in more detail what these mean.

To achieve the overall risk rating, the likelihood and the impact are multiplied to give a score from 1 to 25.

1 is a very low risk; 25 is a very high risk. Risks can be RAG rated:

Risk Scale



Consequence					
5	🟩	🟧	🟥	🟥	🟥
4	🟩	🟧	🟧	🟥	🟥
3	🟩	🟩	🟧	🟧	🟥
2	🟩	🟩	🟩	🟧	🟧
1	🟩	🟩	🟩	🟩	🟩
	1	2	3	4	5
	Likelihood				

When you describe your risk you should ensure you describe it in terms of cause, event and effect.

Remember a risk's score must be kept under review and can go up and down throughout a project or programme. This will be particularly relevant when there are changes to information assets.

Risks will be one or more of:

- Clinical – patients may not engage with services if they feel their information is not secure; or inaccurate information could have a negative impact on patients' individual care
- Reputational – of the CCG gains a reputation for poor information governance key stakeholders may be reluctant to engage with our projects and programmes. We must also never forget poor information management can lead to patient distress.
- Financial – poor information governance may lead to additional spend to address problems or a fine from the Information Commissioner of up to £500,000

Each risk must identify who the lead for managing the risk is, and that person is responsible for keeping the risk under review and getting assurance on the management of the risk.

b. Mitigating and Assuring a Risk

You can never completely get rid of a risk; nor is it appropriate to simply pass it on. When you mitigate a risk, you seek to reduce the likelihood and if possible the impact. Methods for this include: risk reduction; risk retention; risk avoidance; and risk sharing.

Whatever approach you take you must aim to:

- protect the CCG, patients and member practices from information risks;
- support risks being identified, considered and addressed in key approval, review and control processes;
- encourage pro-active rather than re-active risk management;
- support informed decision making throughout the CCG;
- meet legal or statutory requirements; and
- assist in safeguarding the CCG's information assets.

Once you have identified your mitigation (how you make the risk better) you need to identify your assurance by getting sign-off from an appropriate decision making body or senior manager who can ensure the risk is managed well.

Example of mitigation that can be adapted for risk management include:

- identifying information assets and keeping registers up to date;
- ensuring information governance is built into project and programme start-up;
- involving the Caldicott Guardian, SIRO or information governance lead;
- identifying the training needs of staff and colleagues involved in your work;
- ensuring contractors and other stakeholders have good information governance systems in place;
- being clear about the roles, responsibilities, and accountabilities of all involved;
- supporting the CCG's culture of engagement and building relationships with data owners, controllers and users;
- ensuring you abide by the data protection and Caldicott principles;
- taking extra steps to restrict access to data and ensure data security.

5. The CCG's Corporate Risk Register and Risk Management

The CCG has a corporate risk register which discusses information governance, informatices and the handling of data. The Risk Register is discussed at Executive Management Team, Audit Committee (which has overall responsibility for information governance) and the Governing Body.

6. Resources for risk assessment

At the time of writing the lead for information governance is qualified to practitioner level in the management of risk. In addition the Senior Information Risk Officer and the Caldicott Guardian will be able to provide advice and support. For advice on the technical aspects of information security colleagues at the Commissioning Support Unit's IT team will be able to provide advice.

7. References

Health and Social Care Information Centre guidance on risk
http://systems.hscic.gov.uk/infogov/security/risk/inforiskmgtgpg.pdf

8. Dissemination

This guidance is part of the suite of information governance policies and guidance that are on the intranet available for all staff to access. Staff are directed to these policies and guidance as part of their induction and in-house information governance training.