Hampshire, Southampton and Isle of Wight
Clinical Commissioning Group

INFORMATION RISK MANAGEMENT PROGRAMME

Policy number	IG/011/V1.3
Version	1.3
Approved by	Policy Sub Group
Document author	SCW CSU Information Governance Services
Executive lead	Chief Finance Officer (Senior Information Risk Owner)
Date of approval	23 September 2021
Next due for review	April 2023

Version control sheet

Version	Date	Author	Comment
V1.0	15/02/21	Hayley Matthews	Review and update in line with planned merger of HIOW Partnership of CCGs, West Hampshire CCG and Southampton City CCG to form NHS Hampshire, Southampton and Isle of Wight CCG on 1 April 2021. Update includes removal of EU GDPR, replaced with UK GDPR.
V1.1	13/05/21	IG Transition Group	Amendments recommended by the IG Transition Group.
V1.2	07/09/21	Hayley Matthews	Amendments following discussion with CCG governance team.
V1.3	24/09/21	Governance Manager	Reformatted into CCG policy template.

Contents

1. Introduction and purpose

Information is a vital asset and is integral to governance, service planning and delivery, and performance management. To help ensure the safety and security of information within the organisation it is essential that information risk management is not considered in isolation but embedded into all business processes and functions.

Risk management is the recognition and effective management of all threats and opportunities that may have an impact on the organisation's reputation, its ability to deliver its statutory responsibilities and the achievement of its objectives and values.

It is critical that information risk be managed in a structured and robust way across all departments, with each department taking responsibility for information risk. Assets must be identified and ownership at senior staff level assigned. The basis of this approach is documented within the organisation's Information Governance Framework which is updated annually.

The purpose of this document is to establish relevant lines of responsibility and conduct for all members of staff regarding information risk management.

As part of the CCG's overarching Information Governance Rramework and policy, the Information Risk Management Programme supports the CCG in ensuring that:

- Information is protected against unauthorised access
- Confidentiality of information is assured
- Integrity of information is maintained
- Regulatory requirements and legislation are met
- ICT systems are used in such a way as to prevent the 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 authorised to see it
- All breaches of information security, actual or suspected, are reported to, investigated and reported using the Information Governance Incident Management and Reporting Procedures
- Information Governance training is available to all staff via Consult OD website.

2. Scope and definitions

Scope

This document applies to all staff (which include temporary staff, contractors and seconded staff) and external staff/organisations providing services to the organisation by way of a Service Specification or other agreement.

Definitions

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 intentionally or accidentally.

Risk: The chance (probability) of something happening which will impact in an adverse way something of value. This may be damage to information or reputation, or may involve injury or liability. In this context risk is measured as a product of "consequence" x "likelihood" which are given numerical values as will be explained below.

Consequence: The result of a risk becoming a reality. For example, resulting in injury, financial loss, damage. There may be more than one consequence for each risk occurring.

Likelihood: What is the possibility of the risk actually occurring (becoming an issue).

Assessment: The process of identifying and evaluating risks.

Management: In this context, the management of the risk processes within an organisation.

Treatment: Ways of mitigating risk. General risks mitigation involves avoidance, reduction of the risk (consequence, likelihood or both), transfer the risk to someone else, accept the risk.

3. Details of the programme

The CCG has implemented a structured information risk assessment programme. As a minimum all information assets and flows listed in the organisation's Information Asset Registers (IAR) and Data Flow Maps (DFM) will be subject to an annual information risk assessment and review as detailed and evidenced in the IAR and DFMs.

All assets identified in the IARs as 'business critical' (i.e. fundamental to the delivery of the organisation's business) will be subject to a more formal risk assessment and details of the mitigating controls documented and their effectiveness tested in relevant Business Continuity Plans (BCPs) and System Level Security Policies (SLSP).

Risks to Personal Confidential Data (PCD) that arise as a consequence of changes to or the introduction of new systems/process will be identified via the completion of a Data Protection Impact Assessment (DPIA) which identifies and mitigates information risks. DPIAs are formally reviewed by the SCW CSU Senior Information Governance Consultant for the CCG with support provided to the Data Protection Officer (DPO) if requested. DPIAs are

approved by the Senior Information Risk Owner (SIRO) or Caldicott Guardian. Information Assets identified during this process will be included in the IAR and DFM documents. Risks identified as part of the business of the CCG and not through DPIAs will be raised through the organisation's Risk Management Policy.

3.1 Information Asset Owner (IAO) and Data Custodian (DC) work programme

The SCW CSU IG Team will support an annual work programme of related activities in order to produce a documented risk report for the SIRO. IAOs will sign off the activities undertaken in the annual work programme.

Alongside the work programme, the SCW CSU Cyber Security Manager, will ensure that an information security risk assessment and management process is in place to identify, implement and manage controls in place to reduce risk to the CCG's systems and information assets and those managed by SCW CSU on behalf of SCW CSU Customers.

3.2 Information risk management process

All information risks will be recorded, managed and escalated in accordance with the CCG Risk Management Policy and Procedure.

On the identification of a potential risk, a discussion will be held with the DPO to determine the likelihood, consequence and the treatment of the risk. Risks will be managed as follows:

A – Local level management. The risk will be identified as part of team/Directorate risk register or asset register.

B – SIRO managed. The risk will be listed as part of the SIRO IG risk register (Finance register).

3.3 Data Protection Impact Assessments (DPIA)

The UK General Data Protection Regulation (UK GDPR) sets out an obligation to complete a DPIA before carrying out types of processing likely to result in high risk to individuals' interests. This is a key element of the new focus on accountability and data protection by design. DPIAs are mandatory in some cases, and there are specific legal requirements for content and process.

A DPIA is a way to systematically and comprehensively analyse processing activities and help identify and minimise data protection risks. DPIAs should consider compliance risks, but also broader risks to the rights and freedoms of individuals, including the potential for any significant social or economic disadvantage. The focus is on the potential for harm - to individuals or to society at large, whether it is physical, material or non-material.

To assess the level of risk, a DPIA must consider both the likelihood and the severity of any impact on individuals. A DPIA does not have to eradicate the risks altogether, but should help to minimise risks and assess whether or not remaining risks are justified.

DPIAs are a legal requirement for processing that is likely to be high risk. But an effective DPIA can also bring broader compliance, financial and reputational benefits, helping demonstrate accountability and building trust and engagement with individuals.

A DPIA may cover a single processing operation or a group of similar processing operations. A group of controllers can do a joint DPIA.

It's important to embed DPIAs into organisational processes and ensure the outcome can influence plans. A DPIA is not a one-off exercise and should be seen as an ongoing process, and regularly review it.

SCW CSU has produced a comprehensive template and guidance document that form part of a DPIA framework, and this has been adopted for use by the CCG.

3.4 Monitoring and further mitigation of risk

In line with the CCG's Risk Management Policy and Procedure, the following actions are implemented to ensure there is a regular review:

- Monitoring of information security and risk processes through the relevant requirements in the current version of the NHS Digital Data Security and Protection (self-assessment) Toolkit
- Regular review and audit of information flows to ensure confidential information is being transferred securely and in order to reduce information risk
- Implementation of actions plans or internal or external auditor reports
- Analysis of information incidents will support the CCG in understanding the real level of risk being experienced and in adjusting the controls in place.

4. Roles and responsibilities

The CCG has a responsibility for ensuring that it meets its corporate and legal responsibilities and for the adoption of internal and external governance requirements. The CCG Executive Team is also responsible for ensuring that sufficient resources are provided to support the requirements of the programme.

The Management roles are detailed in the Information Governance Management and Strategy document, however key roles are included below:

4.1 Senior Information Risk Owner

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 organisation.

The SIRO has responsibilities to:

- Take ownership of the information risk assessment and risk management process
- Review and agree actions in respect of identified information risks
- Ensure that the organisational 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 the Executive Team are adequately briefed on information risk issues.

4.2 Data Protection Officer

The Data Protection Officer (DPO) should report directly to the CCG Audit and Risk Committee in matters relating to data protection assurance and compliance, without prior oversight by their line manager.

The DPO must ensure that their responsibilities are not influenced in any way, and should a potential conflict of interest arise report this to the highest management level.

The DPOs cannot hold a position within the organisation that can be considered a key decision maker in relation to what personal data is collected and used. Their primary duties are to

- Inform and advise organisation and staff of their IG responsibilities
- Monitor compliance with the UK GDPR and the Data Protection Act (DPA) 2018
- Provide advice where requested regarding the Data Protection Impact Assessment, and monitor performance
- Cooperate with the supervisory authority
- Be the contact point with the Information Commissioners Office (ICO)
- Ensure that where an incident is likely to result in a risk to the rights and freedoms of Data Subjects that the ICO is informed no later than 72 hours after the organisation becomes aware of the incident.

They must give due regard to the risks associated with the processing of data undertaken by the organisation and work with the SIRO and Caldicott Guardian to achieve this.

4.3 Information Asset Owners (IAOs)

Provide 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 are responsible for. They will also investigate and take action on any potential breaches of the organisations

policies and procedures, and ensure that a Data Protection Impact Assessment (DPIA) is undertaken where appropriate.

4.4 Data Custodian (DCs)

Recognise actual and potential security incidents and consult the appropriate IAO on incident management. Ensure their directorate's Information Asset Registers and Data Flow Mapping sheets are accurate and up to date and identify any actual or potential risks that need further consideration by the IAO/SIRO.

4.5 SCW CSU Cyber Security Manager

Will ensure security accreditation of information systems in line with the organisation's approved definitions of risk and that all arrangements for managing information security are effective and aligned with the organisation's Information Security Management System (ISMS) and Risk Policies. They will develop and maintain an information security assurance plan to ensure the appropriate management and prioritisation of risks. They co-ordinate the necessary response and resolution activities following a suspected or actual security incident or breach, keeping the information risk lead (SIRO) and IAOs informed of security incidents, impacts and causes, resulting actions and learning outcomes.

4.6 All Staff

All staff have a legal duty of confidence to keep PCD and commercially confidential information secure and private, and not to divulge information accidentally. Staff may be held personally liable for a breach of confidence and should ensure that:

- Confidential information is kept secure and only accessed on a need–to-know basis
- Adhere to all the risk and incident reporting policies/procedures
- Bring to their line managers any concerns regarding information governance and risk.

5. Equality Analysis

The CCG is committed to equality, diversity and inclusion for all, as well as to meeting the Public Sector Equality Duty (Equality Act 2010).

Both new policies and existing policies and frameworks when reviewed, come within the Public Sector Equality Duty. This means that authors must consider whether the policy / framework will be effective for all patients and/or staff. This process is called equality impact assessment.

This document has been assessed as having a low impact on people with characteristics protected by the Equality Act. As such a full equality impact assessment is not required.

However, each policy which underpins this programme which has been assessed as having a high or medium equality impact has been fully assessed using the CCG Equality Impact Assessment template.

6. Training

All staff will undertake Data Security Awareness (previously Information Governance) training via the ConsultOD website (here) or where appropriate and agreed via face to face training sessions. Extra training will be given to those who need it such as IAOs/DCs and those dealing with requests for information.

All staff are made aware of what could be classed as an information security incident or breach of confidentiality. They are made aware of the process to follow and the forms to complete, so that incidents can be identified, reported, monitored and investigated.

There is an extensive guidance document that accompanies the DPIA template that enables staff to understand the types of information risk that can occur and encourage them to embed a 'privacy by design and default' approach at the beginning of new projects and activities.

7. Dissemination/publication

This policy will be made available to staff on the Information Governance page of the CCG website, with a link to the appropriate page also available on the staff intranet / StayConnected Portal.

8. Monitoring compliance and effectiveness

The performance of the information risk management programme will be monitored in two ways:

- Against the criteria set in the Data Security and Protection Toolkit using the annual submission on 31 March and associated improvement plan
- The internal audit process and subsequent report to the Audit and Risk Committee.

9. Review

This programme will be reviewed every two years or sooner due to legislation changes.

10. Stakeholder /consultation information

This policy was already in place in the Hampshire & Isle of Wight Partnership of CCGs, West Hampshire CCG and Southampton City CCG prior to the merger to form NHS Hampshire, Southampton and Isle of Wight CCG on 1 April 2021.

It has been through an internal process and reviewed by the Information Governance Team, South Central & West Commissioning Support Unit, with input from the IG Transition Group, DPO, Governance Managers and reviewed by the SIRO.

11. References and associated documents

- Information Governance Framework
- Information Governance Policy
- Confidentiality and Safe Haven Policy
- SCW CSU Network Security Policy
- SCW CSU IT Security Framework
- SCW CSU Information Security Policy
- SCW CSU DPIA Framework and Guidance
- SCW CSU Security Incident Handling Policy
- Information Governance Incident Management and Reporting Procedure
- CCG Corporate Risk Management Policy
- Data Security Standards for Health and Care.