Hampshire and Isle of Wight
Partnership of Clinical Commissioning Groups

Information Risk Management Programme

Version 3 August 2020

Version Number: 3	Issue/approval date: August 2020
Status: Final	Next review date: 01-04-2021

Hampshire and Isle of Wight
Partnership of Clinical Commissioning Groups

DOCUMENT CONTROL

Document Name	Version	Status	Author
Information Risk Management Programme	*3*	*Final*	*Various*
Document objectives:	*This document identifies the measures taken to ensure that the H&IoW Partnership of CCG approaches information risk in a planned and managed way*		
Target audience:	*All staff*		
Committee/Group Consulted:	*Information Governance Steering Group* *Corporate Governance & Assurance Group*		
Monitoring arrangements and indicators:	***Annual review***		
Training/resource implications:	*Already included in training provided*		
Approved and ratified by:	*Information Governance Steering Group* *Corporate Governance & Assurance Group*	*Date: 16/08/18* *Date: 07/09/18*	
H&IoW Partnership of CCG Approved		Date	
Equality Impact Assessment:	*Not applicable*	*Date: NA*	
Date issued:	*August 2020*		
Review date:	*01 April 2021*		
Author:	*Senior Information Governance Manager- SCW*		
SCW Lead Director:	*Head of Information Governance - SCW*		
H&IoW Partnership of CCG Lead Director:	*Director of Finance & SIRO*		

Version Control

Change Record

Date	Author	Version	Page	Reason for Change
29-06-18	A. Sumner	2.0	All	Legislative changes
22-05-19	A. Sumner	2.1	All	Reset of review date pending Brexit agreement
25-06-19	M. Wall	2.1	Various	Document updated to reflect alignment of policies across the H&IoW Partnership of CCG, inserted Partnership description under section 1
03/12/2019	L. Long	2.2		Removal of NEHF CCG from Partnership
21/8/20	L.Long	2.2	Page 2	Review date extended to April 2021

Reviewers/contributors

Name	Position	Version Reviewed & Date
Angela Sumner	SCW Senior IG Manager	V2.1 22-05-19
Matt Wall	SCW IG Manager	V2.1 25/06/2019
Lucy Long	**SCW IG Manager**	**V2.2 03/12/19**

Contents

Version Number: 3	Issue/approval date: August 2020
Status: Final	Next review date: 01-04-2021

1. Introduction and Purpose

This policy applies to all Clinical Commissioning Groups, hereafter 'the CCG', who are part of the Hampshire and Isle of Wight Partnership of CCGs, hereafter 'the partnership' The Hampshire and Isle of Wight Partnership of CCGs is comprised of North Hampshire CCG; Fareham & Gosport CCG; South Eastern Hampshire CCG and Isle of Wight CCG. All CCGs in the Partnership will adhere to the individual legal and statutory obligations of their respective organisations.

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 Partnership's overarching information governance framework and policy, the Information Risk Management Programme supports the individual CCG's 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 Incident Management and Reporting Procedures
- Information Governance training is available to all staff via Consult OD website

2. Scope and Definitions

2.1 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.

2.2 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 Register (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 IAR 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 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. DPIA's are formally reviewed by the SCW IG review panel (where requested) and approved by the Caldicott Guardian/SIRO. 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 Policy.

3.1 IAO and Data Custodian Work Programme

The SCW 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 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 on behalf of SCW 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 Data Protection Officer 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).
C – Executive Management Team oversight. The risk will be included as part of the Corporate Governance and Assurance Framework process and risk register.

3.4 Data Protection Impact Assessments (DPIA)

The General Data Protection Regulation introduces a new 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 now 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 has produced a comprehensive template and guidance document that form part of a DPIA framework and is available to the CCG to adopt and use.

3.5 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 Partnership Executive Management 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 Framework 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's have 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 Management Team are adequately briefed on information risk issues

4.2 Data Protection Officer

The Data Protection Officer (DPO) should report directly to the Hampshire and Isle of Wight Partnership Audit Committees meeting in common and Partnership Governing Bodies meeting in common 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 GDPR and the 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
- ✓ 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 Custodians

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

They 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 Information Asset Owners 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. Training

All staff will undertake Data Security Awareness (previously Information Governance) training via the Consult OD 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/Data Custodians 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.

6. Review

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

7. References and Associated Documents

- Information Governance Framework
- Information Governance Policy
- Confidentiality and Safe Haven Policy
- SCW Network Security Policy
- SCW IT Security Framework
- SCW Information Security Policy
- SCW DPIA Framework and Guidance
- SCW Security Incident Handling Policy
- Information Governance Incident Management and Reporting Procedure

Data Security Standards for Health and Care