NHS
Bristol, North Somerset and South Gloucestershire
Clinical Commissioning Group

Information Risk Management Process

Shaping better health

Please complete the table below: *To be added by corporate team once policy approved and before placing on website*	
Policy ref no:	To be filled in by Corporate Services
Responsible Executive Director:	Sarah Truelove
Author and Job Title:	Information Governance Team, SCW CSU
Date Approved:	11th May 2022
Approved by:	Sarah Truelove
Date of next review:	May 2024

Table of Contents

Table of Contents 2

1 Introduction 4

1.1 BNSSG CCG Values 4

2 Purpose and scope 4

2.1 Purpose 4

2.2 Scope 5

3 Duties – legal framework for this policy 5

4 Responsibilities and Accountabilities 6

4.1 Senior Information Risk Owner 6

4.2 Caldicott Guardian 6

4.3 Data Protection Officer 6

4.4 Information Asset Owners (IAOs) 7

4.5 Information Asset Administrators (IAAs) 7

4.6 All Staff 7

5 Definitions/explanations of terms used 7

6 Details of the Process 8

6.1 IAO and IAA Work Programme 8

6.2 Data Protection Impact Assessments (DPIA) 9

6.3 Information Risk Management Process 9

7 Training requirements 10

8 Implementation and Monitoring Compliance and Effectiveness 10

9 Countering Fraud 10

10 References, acknowledgements and associated documents 10

Information Risk Management Process

1 Introduction

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 Strategy and Framework. This document must be read in conjunction with the following policies:

Information Governance Policy

Acceptable use of IT policy

Records Management Policy

1.1 BNSSG CCG Values

Ensuring that we and protect information and manage information risks ensures the confidentiality, integrity and availability of the information that we rely on. This support our core values of being able to act with integrity, work better together and to do the right thing.

2 Purpose and scope

2.1 Purpose

The purpose of this document is to establish relevant lines of responsibility and conduct for all members of staff regarding information risk management. There are many types of information which require risk management including: personal

information regarding staff and patients; commercially sensitive contracts and negotiations; procurement information.

As part of the organisation's overarching information governance framework and policy, the Information Risk Management Process supports BNSSG 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 CCG's Incident Management and Reporting Procedures
- Information Governance training, called Data Security Awareness is available to all staff via the Consult OD website

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 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.

This process will be reviewed every two years or where required more frequently.

3 Duties – legal framework for this policy

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 Directors are responsible for ensuring that sufficient resources are available to support the requirements of information risk management within directorates.

4 Responsibilities and Accountabilities

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 responsibility to:

- Take ownership of the information risk assessment and information 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 Caldicott Guardian

The Caldicott Guardian has responsibility for ensuring that clinical information is appropriately managed and may be required to support the management and assessment of associated information risks

4.3 Data Protection Officer

The Data Protection Officer (DPO) should report directly to the Governing Body 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 for Information Governance breaches and incidents.
- Ensure that where an incident is likely to result in a risk to the rights and freedoms (as defined in GDPR) 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.

4.4 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. This is in part through the regular review of Information Asset Registers and Data Flow Maps. 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.

4.5 Information Asset Administrators (IAAs)

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.

4.6 All Staff

All staff have a legal duty of confidentiality to keep personal information 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:

- They comply with all policies, guidance and arrangements for using information appropriately and for keeping it secure.
- Undertaking all relevant training associated with role.
- 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
- They are aware of what could be classed as an information security incident or breach of confidentiality and know the process to follow and the forms to complete, so that incidents can be identified, reported, monitored and investigated.

5 Definitions/explanations of terms used

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 or 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.

6 Details of the Process

The CCG has implemented a structured information risk assessment programme. This involves all information assets and flows being listed in the organisation's Information Asset Register (IAR) and Data Flow Maps (DFM). This ensures that the organisation understands what information is being held, where it is stored, how it is accessed and how it is shared. The IAR and DFM will be subject to an annual review and risk assessment.

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 and approved by the CCG's Caldicott Guardian/SIRO. Information Assets identified during this process will be included in the IAR and DFM documents.

6.1 IAO and IAA Work Programme

The SCW IG Team will support an annual work programme of related activities in order to produce a documented information risk report for the SIRO. IAOs will support 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 managed by SCW.

6.2 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. See separate document/guidance on the use of DPIAs

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.

6.3 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. High Risks will be included in the Corporate Risk Register.

7 Training requirements

All staff will undertake Information Governance training called Data Security Awareness via the Consult OD link or where appropriate and agreed via face to face training sessions. Extra training will be given to those who need it such as IAOs/IAAs and those dealing with requests for information. Support is available from the CSU IG team

8 Implementation and Monitoring Compliance and Effectiveness

The following actions are implemented to ensure there is a regular review of information risk; these activities are all under the oversight of the Information Governance Group:

- Monitoring of information security and risk processes through the CCG's Data Security and Protection Toolkit Submission. This is overseen by the SIRO.
- Regular review and audit of information flows to ensure confidential information is being transferred securely and in order to reduce information risk. This is co-ordinated by the Information Governance Manager and completed by Information Asset Owners.
- 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

9 Countering Fraud

The CCG is committed to reducing fraud in the NHS to a minimum, keeping it at that level and putting funds stolen through fraud back into patient care. Therefore, we have given consideration to fraud and corruption that may occur in this area and our responses to these acts during the development of this policy document.

10 References, acknowledgements and associated documents

- CCG Information Governance Framework
- CCG Information Governance Policy
- CCG Confidentiality and Security of Information Policy
- SCW IT Policies
- CCG DPIA Framework and Guidance
- CCG Incident Reporting Process