Working with you to make Sheffield HEALTHIER

NHS Sheffield Clinical Commissioning Group

INFORMATION ASSET RISK MANAGEMENT PLAN

January 2021

Version:	V2.0
Policy Number:	CO029/01/2023
Date ratified:	12 February 2021
Name of originator/author:	IG Manager
Sponsor:	Deputy Director of Information, Performance and PMO
Name of responsible committee	Governance Sub-committee
Date issued:	February 2021
Review date:	January 2023

MINDFUL EMPLOYER

disability confident EMPLOYER

Version Control

VERSION CONTROL				
Version	**Date**	**Author**	**Status**	**Comment**
1.0		**G.Nubour**	**REVIEW**	**Renamed slightly and restarted version number** **Adapted to reflect DPA2018/ GDPR** **Quaterly Reviews of IAR / Datafows** **72 Hour incident reporting requirement added** **Changed to 2 year review schedule** **Format adapted to one of a procedure, two sections removed** **Removed Appendix B**
2.0	**Jan 2021**	**G.Nubour**	**Review**	**Included reference to Data Processors** **Other Minor Revisions**

Contents

1 Introduction and Purpose

Information and information systems are important corporate assets and it is essential to take all the necessary steps to ensure that they are at all times protected, available and accurate to support the operation and continued success of the CCG.

There needs to be a comprehensive programme of activity across the CCG to identify information risks and manage them effectively.

A number of key activities in the Information Governance toolkit form the basis of building an information risk framework, namely:

- Mapping flows of information
- Identifying and maintaining a register of key information assets
- Completion of confidentiality audits
- Setting out continuity plans for periods of information unavailability

2 Information Security Management Roles and Responsibilities

The key requirement is for information risk to be managed in a robust way within all work areas and not be seen as something that is the sole responsibility of IT or IG staff. Assurances need to be provided in a consistent manner. To achieve this, a structured approach is needed, building upon the existing information governance framework within which many parts of the NHS are already working. This structured approach relies upon the identification of information assets and assigning 'ownership' of assets to senior accountable staff, ensuring all staff understand their roles and responsibilities in relation to managing information risk.

Chief Officer	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.
Senior Information Risk Owner (SIRO)	The SIRO is an executive who is familiar with and takes ownership of the organisation's information risk policy, acts as advocate for information risk for the Governing Bodies.
Information Asset Owner (IAO)	Information Asset Owners are senior individuals involved in running the relevant business. 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.
Information Asset Administrator (IAA)	Information Asset Administrators ensure that policies and procedures are followed, recognise actual or potential security incidents, consult their IAO on incident management, and ensure that information asset registers are accurate and up to date.
All Staff	Everyone has a role in the effective management of information risk. All staff will actively participate in identifying potential information risks in their area and contribute to the implementation of appropriate treatment actions.

3 Definitions

IAA Information Asset Administrator
IAO Information Asset Owner
ICO Information Commissioner's Office
IG Information Governance
PCD Personal Confidential Data
SIRO Senior Information Risk Owner
SLSP System Level Security Policy
MOU Memorandum of Understanding

4 Process/Requirements

The Information Asset Risk Management Process

The Information Risk Management System Process will be developed to encompass:

- Information Asset Register (including risk assessments)
- Data Flow Mapping (Identifying Exchanges of Personal Confidential Data)
- Identification of critical assets (business impact assessment)

Identifying Information Assets

Information assets come in many shapes and forms. Therefore, the following list can only be illustrative. It is generally sensible to group information assets in a logical manner e.g. where they all related to the same information system or business process. Information assets are identifiable and definable assets owned or contracted by an organisation which are 'valuable' to the business of that organisation, such as:

- databases
- data files
- contracts and agreements
- IT systems which support information processing
- system documentation
- research information
- training records and materials
- operational/ support procedures
- business continuity plans
- archived information

Information assets could be kept in a variety of formats and on a variety of media, e.g. paper, x-ray film, network folders, CD-ROMS, backup tapes etc.

Examples of paper information assets include:

- patient records
- personnel files
- letters
- funding requests

- collated sickness absence returns
- expenses
- corporate records

Examples of electronic assets include:

- annual leave/ sickness records
- electronic orders, contracts or agreements
- local databases
- scanned document archive
- electronic copies of letters/meeting papers

Information assets may contain personal confidential data or commercially sensitive information. Priority will be given to information assets that comprise or contain personal information about patients or staff**.**

All organisations are subject to change brought about by modifications to the operational and technical environments. These in turn change the information assets held by the organisation and the risks associated with them, resulting in a requirement to periodically review any previously recorded information assets and risk assessments.

The UK General Data Protection Regulation and Data Protection Act 2018 (UK GDPR and DPA) require organisations to maintain accurate and up to date records of processing. Consequently, the CCG has decided to undertake formal quarterly information asset register reviews, to be carried out by IAOs with assistance from IAAs.

Mapping Flows of Personal Confidential Data - Dataflows

To adequately protect personal information, organisations need to know how information is transferred into and out of the organisation, risk assess the transfer methods and consider the sensitivity of the information being transferred. Transfers of all personal and sensitive information must comply with professional standards and relevant legislation (such as Article 5 of the GDPR) which requires appropriate technical and organisational measures to be taken against unauthorised or unlawful processing of, and accidental loss or destruction of, or damage, to personal data.

To ensure all transfers of personal confidential data (PCD) are identified, the CCG must determine where, why, how and with whom it exchanges information. This is known as data flow mapping and the information recorded in the Information Asset Register allows the identification of all assets of which part or all of their content are sent or received either internally or externally to the CCG.

As with the Information Asset Register, dataflows are subject to change and should therefore be regularly reviewed. As such formal reviews will be conducted quarterly by IAOs.

Annual Information Risk Management Activities

The Information Asset Risk Management plan has been created to support the activities outlined below, to enable the CCGs to identify information risks and manage them effectively. Activities include:

- Identify all Information Assets and their owners (IAOs)
- Populate of the Information Asset Register

- Identify any 3rd party access and review contractual arrangements
- Ensure all Data Processors have formal contracts or MOUs in places with adequate data protection clauses
- Ensure IAOs are adequately trained to fulfil their duties
- Risk Assessments for all information assets on the Information Asset Register.
- Identification of “business critical” assets and review business continuity plans.
- Undertake dataflow mapping exercise to identify all exchanges of PCD
- Risk assessments of dataflows
- Development of confidentiality audit procedures
- Provide SIRO with highlight and completion reports
- IG Work Programme

Information Incident Reporting

Damage resulting from potential and actual information security events should be minimised and lessons learnt from them with relevant processes scrutinised. All information security incidents, including cyber security incidents, (including but not limited to, physical destruction or damage to the organisation's computer systems, loss of systems availability and the theft, disclosure or modification of information due to intentional or accidental unauthorised actions) suspected or observed, should be reported through the CCG's incident reporting system and managed in line with the incident reporting procedures and Risk Management Strategy. Significant or serious incidents will need to be reported to the ICO and other regulatory bodies within 72 hours of discovery.

Confidentiality Audits

The IG Toolkit requires that CCGs ensure access to confidential personal information is monitored and audited locally, and in particular ensure that there are agreed procedures for investigating confidentiality events.

The CCGs must have a process to highlight actual or potential confidentiality breaches, particularly where person identifiable information is held and must also have procedures in place to evaluate the effectiveness of controls within these systems.

Confidentiality audits will focus primarily on controls within electronic records management systems, but should not exclude paper record systems: the purpose being to discover whether confidentiality has been breached, or put at risk through deliberate misuse of systems, or as a result of weak, non-existent or poorly applied controls.

A Confidentiality Audit Procedure will be developed and all work areas within the CCG, which process (handle) personal confidential data (both patient and staff information) will be subject to the confidentiality audit procedures.

Information Risk Management Training

The IG Team will make training available to Information Asset Owners and Information Asset Administrators to enable them to fulfil their responsibilities. The training will provide an understanding of why the SIRO role has been introduced and what the roles of SIRO, IAO and IAA involve. An overview of what information assets are and how they are to be recorded and risk assessed and maintained in the Information Asset Register will be given.

The SIRO will also be required to successfully complete strategic information risk management training at least annually.

Assurance Reporting

The SIRO will receive, highlight and complete a report as part of the Information Risk Management work package highlight any information risks across the CCG. Details of any IG Security Incidents will be included in the IG Update report for the appropriate governance group. Annually, a 12 month report will be submitted by the SIRO to provide the Governing Bodies with assurances of the progress and developments within Information Governance.

5 References and links to other documents

Information risk management is a component of information governance and all staff should be made familiar with the CCGs IG policies available on the intranet

Data Security Standard 01: Personal confidential data big picture guide https://www.dsptoolkit.nhs.uk/Help/23 (an overview of information assets risk assessment and dataflows

6 Review

This plan and will be reviewed every two years or earlier depending on changes in local or national requirements.

Appendix A. Information Risk Management Activities Plan

Stage	Information Risk Management Task	Deliverables
1.0	Preparation/review of key documents	Up to date template documents ensuring IG Toolkit compliance
1.1	Review information asset register	Initial revised Information Asset Register
1.2	Provide training to IAOs	IAO training sessions Training attendance records
1.3	Liaise with relevant staff to update and validate Information Asset Register and identify flows of personal information	Current completed Information Asset Register with all new assets listed Returned dataflows
1.4	Information Asset and Dataflow mapping chase-up	
1.5	Develop SLSP's with Asset Owners	Completed System Level Security Policies
1.6	Identify any 3rd parties (contractors/support organisations) with access to any information assets and review IG clauses in relevant contracts	Third parties identified and logged in Information Asset Register / SLSP Assurance that 3rd party contracts are robust in terms of IG
1.7	Support Asset Owners to carry out risk assessments and confidentiality audits of assets.	Completed risk assessments and confidentiality audits
1.8	Put systems in place to maintain the Information Asset Register	Regularly updated Information Asset Register
1.9	Collate and analyse findings from the risk assessments and confidentiality audits.	List of findings from risk assessments List of confidentiality audit findings
2.0	Identify gaps in compliance and support IAO's to deliver improvements	List of agreed documented actions produced by IAOs Entries on risk register if appropriate
2.1	Report findings to IG leads, SIRO's and relevant groups/committees	Highlight reports of findings and actions required to mitigate any issues
2.2	Support staff in implementing remedial actions	Achievable risk management action plans
2.3	Completion report	Completion report