Thinking Differently

NHS
Dudley
Clinical Commissioning Group

INFORMATION RISK MANAGEMENT POLICY

UNIQUE REF NUMBER:	**AC/IG/015/V2.0**
DOCUMENT STATUS:	**APPROVED BY AUDIT & GOVERNANCE – 18 OCTOBER 2018**
DATE ISSUED:	**NOVEMBER 2018**
DATE TO BE REVIEWED:	**NOVEMBER 2021**

AMENDMENT HISTORY

VERSION	DATE	AMENDMENT HISTORY
V1	June 2013	Version approved by Audit Committee 19 June 2013
AC/IG/015/V1.1	December 2013	Addition of branding and formatting changes in line with Policy for Development of Policies
AC/IG/015/V1.2	February 2014	Addition of unique reference number prior to publication
AC/IG/010/V2.0	September 2018	Reviewed extensively in line with Arden & GEM CSU Policy and changes to UK Data Protection Legislation

REVIEWERS

NAME	DATE	TITLE/RESPONSIBILITY	VERSION
Donna Dallaway	June 2013	CSU Information Governance Manager	V1
Matthew Hartland	June 2013	Chief Finance Officer	V1
Julia Dixon	June 2013	Staff Side Representative	V1
Kelly Huckvale	September 2018	Information Governance Officer, Arden & GEM CSU	V2.0

APPROVALS
This document has been approved by:

NAME	DATE	VERSION
CCG Audit Committee	19 June 2013	V1
Audit & Governance Committee	18 October 2018	V2.0

NB: The version of this policy used on the intranet must be a PDF copy of the approved version.

DOCUMENT STATUS
This is a controlled document. Whilst this document may be printed, the electronic version posted on the intranet is the controlled copy. Any printed copies of the document are not controlled.

RELATED DOCUMENTS
These documents will provide additional information:

DOCUMENT TITLE
Dudley CCG Information Asset Register
Dudley CCG Data Flow Mapping Register
Data Protection and Confidentiality Policy
Records Management Policy
Information Governance Policy
Information Security Policy

APPLICABLE LEGISLATION

Data Protection Act 2018
General Data Protection Regulation (GDPR)
Human Rights Act 1998
Freedom of Information Act 2000
Access to Health Records Act 1990 (where not superseded by the Data Protection Act)
Computer Misuse Act
Copyright, Designs and Patient's Act 1998 (as amended by the Copyright Computer Programs Regulations 1992)
Crime and Disorder Act

Electronic Communications Act 2000
Regulatory of Investigatory Powers Act 2000
Common Law Duty of Confidentiality
National Health Service Act 1977

Contents

POLICY OVERVIEW

1.0 Introduction

1.1 In recent years there has been much media interest in the losses of personal confidential data (PCD) across public services, including the NHS. Whilst every technical solution possible can be implemented to protect the data from loss or theft, there is always some loophole whereby data can be lost. Invariably the human element is the weak link with people failing to do what they are required to do, or else doing things they should not be doing i.e. taking either a deliberate or inadvertent risk.

1.2 This policy is aimed at ensuring all risks associated with the use of personal or sensitive information are considered and thereafter managed in such a way as to minimise residual risk. Any serious remaining risk associated with information is reported to the Board via the Corporate Risk Register and the Senior Information Risk Owner (SIRO).

1.3 It should be noted that this policy does not supersede Dudley CCG's Risk Management Policy; rather it defines the specific aspects relating to information. Dudley CCG's Risk Management Policy is still the overarching policy on risk management. The key requirement is for information risk to be managed in a robust way and therefore a structured approach that underpins the existing information governance framework is necessary to provide the required assurances.

2.0 Purpose

2.1 The purpose of this policy is to provide Dudley CCG staff with a framework with regard to Information Risk Management.

2.2 Dudley CCG's Board have approved the introduction and embedding of information risk management into key controls and approval processes of all major business processes and functions of Dudley CCG. This decision reflects the high level of importance placed upon minimising information risk and safeguarding the interests of patients, staff and Dudley CCG itself.

2.3 Information risk is inherent in all administrative and business activities and everyone working for or on behalf of Dudley CCG continuously manages information risk. The Board recognises that the aim of information risk management is not to eliminate risk, but rather to provide the structural means to identify, prioritise and manage the risks involved in all of Dudley CCG's activities. It requires a balance between the cost of managing and treating information risks with the anticipated benefits that will be derived.

2.4 The Board acknowledges that information risk management is an essential element of broader information governance and is an integral part of good management practice. The intent is to embed information risk management in a very practical way into business processes and functions. This is achieved through key approval and review processes/controls – and not to impose risk management as an extra requirement.

3.0 Scope

3.1 This Policy applies to all Dudley CCG staff, including permanent and temporary staff, secondees, contracted staff, students/trainees/apprentices and voluntary workers.

In addition, this Policy applies to all third parties and others authorised to undertake work for an on behalf of Dudley CCG.

4.0 Key Principles

4.1 The Information Risk Management Policy has been created to:

- Protect Dudley CCG, its staff and patients from information risks where the likelihood of occurrence and the consequences are significant
- Provide a consistent risk management framework in which information risks will be identified, considered and addressed in key approval, review and control processes
- Encourage pro-active rather than re-active risk management
- Provide assistance to and improve the quality of decision making throughout Dudley CCG
- Meet legal or statutory requirements
- Assist in safeguarding Dudley CCG's information assets

4.2 The purpose of this Policy is to formally establish Dudley CCG's position regarding its information risk management process. The intent is to embed information risk in a very practical way into business processes and functions via key approval processes, review processes and controls, and not to impose information risk management as an extra requirement.

4.3 This will be undertaken in accordance with Dudley CCG's Risk Management Policy.

5.0 Responsibilities

5.1 The Chief Accountable Officer is the Accountable Officer for Information Security and the system of internal controls.

5.2 The following key roles have responsibility for;

- Overseeing the development of an Information Risk Policy
- Taking ownership of the risk assessment process for information risk, including review of the annual information risk assessment to support and inform the Annual Governance Statement.
- Reviewing and agreeing action in respect of identified information risks
- Ensuring that Dudley CCG's approach to information risk is effective in terms of resource, commitment and execution and that this is communicated to all staff
- Providing a focal point for the resolution and/or discussion of information risk issues
- Ensuring the Board is adequately briefed on information risk issues.

5.3 Senior Information Risk Owner

The Chief Finance Officer is the Senior Information Risk Officer (SIRO) and is responsible for coordinating the development and maintenance of information risk management policies, procedures and standards for Dudley CCG. The SIRO takes ownership of information risk and is a key factor in successfully raising the profile of information risks and to embedding information risk management into Dudley CCG's culture. The SIRO shall advise the Board on all information risk management strategies and provide periodic reports and briefings on progress.

5.4 Information Asset Owner (IAO)

The IAO will typically be the Head of Department where specific systems are used will be responsible for ensuring that this policy is implemented in their department and on

the systems contained therein. They will ensure they have procedures in place which will reduce, mitigate or remove any risk associated with the use of information, particularly patient identifiable data.

IAOs are accountable to the SIRO and will provide assurance that information risk is being identified and managed effectively for those information assets that they have been assigned ownership of.

Dudley CCGs Information Asset Owners (IAOs) shall ensure that information risk assessments are performed at least annually on all information assets where they have been assigned 'ownership', following guidance from the IG Team on assessment method, format, content, and frequency. IAOs shall then submit the risk assessment results and associated mitigation plans to the IG Consultant Hub and IT Security Manager for review, along with details of any assumptions or external dependencies. Mitigation plans shall include specific actions with expected completion dates, as well as an account of residual risks. IAOs will undertake an annual information flow mapping exercise in conjunction with the IG team and from this exercise determine the risks regarding data flows within the organisation and/or with its delivery partners.

5.5 Information Asset Administrator (IAA)

The Information Asset Administrator (IAA) will typically be the member of staff who manages relevant local systems on a day to day basis and is responsible for ensuring system level security policies are in place and through these policies will ensure most risks are mitigated. Any remaining risk will be reported to the Information Asset Owners (IAO) and SIRO.

5.6 Caldicott Guardian

The Clinical Lead for IT has been appointed to the role of Caldicott Guardian and is therefore the Board member responsible for ensuring the confidentiality of patient based information. This was defined in the Caldicott Report of December 1997. The Caldicott Guardian will ensure that there are robust policies in place to ensure that patient information will remain confidential and be seen only by those clinicians authorised to see that data. The Caldicott Guardian will ensure breaches of this policy in respect of patient information are investigated and will also ensure that information governance is duly regarded at Board level when appropriate.

5.7 Information Governance Lead

The Information Governance Lead will, through the Data Security and Protection Toolkit, ensure that Dudley CCG has robust policies, procedures, strategies, training and awareness programmes and monitoring schedules in place to ensure the confidentiality, integrity and availability of data and ensure that Dudley CCG complies with relevant current legislation.

5.8 IT Manager

The IT Manager will ensure that technical solutions are in place to protect all personal and otherwise sensitive electronic information, wherever this information is accessed.

5.9 Responsibilities of all staff

All staff will ensure that they have read this policy and have undertaken relevant mandatory Information Governance applicable to their role.

In addition, all staff will abide by the policies and the procedures, regarding Information Governance ratified by Dudley CCG as well as legislation and law.

6.0 Definitions

Risk	The chance of something happening which will have an impact upon objectives. It is measured in terms of consequence and likelihood
Consequence	The outcome of an event or situation expressed qualitatively or quantitatively, being a loss, injury, disadvantage or gain. There may be a range of possible outcomes associated with an event
Likelihood	A qualitative description or synonym for probability or frequency
Risk Assessment	The overall process of risk analysis and risk evaluation
Risk Management	The culture, processes and structures that are directed towards the effective management of potential opportunities and adverse effects.
Risk Treatment	Selection and implementation of appropriate options for dealing with risk. Conceptually, treatment options will involve one or a combination of the following five strategies: o Avoid the risk o Reduce the likelihood of occurrence o Reduce the consequences of occurrence o Transfer the risk o Retain/accept the risk
Risk Management Treatment	The systematic application of management policies, procedures and practices to the tasks of establishing the context, identifying, analysing, evaluating, treating, monitoring and communicating risk

7.0 Monitoring Compliance

7.1 Staff are expected to comply with the requirements set out within the Information Risk Management Policy and related policies. Compliance will be monitored via Manager and Information Governance Team reports of spot checks, completion of staff questionnaires, incidents reported, electronic audit trails and submission of the Data Security and Protection Toolkit.

7.2 Non-adherence to the Information Risk Management Policy and related policies will result in local disciplinary policies being implemented.