NHS
Bury
Clinical Commissioning Group

Information Risk Policy

Version:	4.0
Ratified by:	NHS Bury Clinical Commissioning Group Information Governance Operational Group
Date ratified:	30th January 2018
Name of originator /author (s):	GMSS Information Governance Team
Responsible Committee / individual:	NHS Bury Clinical Commissioning Group Audit Committee
Date issued:	February 2018
Review date:	February 2020
Target audience:	NHS Bury Clinical Commissioning Group Members, staff, volunteers and contractors
Equality Analysis Assessed:	Yes

Further information regarding this document

Document name	Information Risk Policy CCG.GOV.012.4.0
Category of Document in The Policy Schedule	Governance
Author(s) Contact(s) for further information about this document	GMSS Information Governance Team
This document should be read in conjunction with	All Information Governance Policies
This document has been developed in consultation with	NHS Bury Clinical Commissioning Group Operational Group
Published by	NHS Bury Clinical Commissioning Group 21 Silver Street Bury BL9 0EN Main Telephone Number: 0161 762 3100
Copies of this document are available from	CCG Corporate Office CCG website

Version Control

Version History:		
Version Number	Reviewing Committee / Officer	Date
0.1 = draft 1	NHS Bury CCG Information Governance Operational Group	28th November 2013
1.1 = Policy once ratified	NHS Bury Clinical Commissioning Group	8th January 2014
2.1 = policy once reviewed	NHS Bury Clinical Commissioning Group	10th December 2014
3.0 = policy once reviewed	NHS Bury Clinical Commissioning Group, Quality and Risk Committee	15th February 2016
3.1 = policy once reviewed	GMSS IG Team	20th December 2017
4.0 = policy once ratified	NHS Bury CCG Information Governance Operational Group	30th January 2018

Information Risk Policy

Contents

1. Assurance Statement

This policy lays the Policy for a formal information risk management programme in NHS Bury CCG (referred to as the CCG) by explicitly establishing responsibility for information risk identification and analysis, planning for information risk mitigation, information risk management and its oversight.

The CCG and their management team are required to assure the formal introduction and embedding of information risk management into key controls and approval processes of all major business processes and functions of the organisation.

Information risk is inherent in all administrative and business activities and everyone working for or on behalf of the CCGs continuously manage information risk.

It should be noted that this policy complements and works on the same principle outlined in the CCG's Risk Management Policy. This policy specifically relates to risk associated with management information, records and data.

2. Introduction

Information risk is a factor that exists in all areas where information of a personal or confidential nature are used and managed.

This policy sets out the requirements placed on all staff in the use and management of information and the risks associated with using such information.

The policy takes key areas from the NHS National Patient Safety Agency "Risk Matrix for Risk Managers" and works in conjunction with the Risk Management Policy as well as the Information Governance Policy, Data Protection and Confidentiality Policy and Record Management Policy.

Information risk management is a part of Information Governance (IG) and it is acknowledged that information governance, including the management of information risks become part of the culture of the organisation, ensuring that staff are aware of, and work to, good IG (and therefore information risk) practices.

3. Purpose

The purpose of this policy is to provide a consistent way of managing information risk in the organisation allowing the information to be managed in a way that highlights when information may be at a significantly high risk, thereby providing a layer of protection for patients, staff and the organisation. The highlighting of risk will then allow risks to be properly addressed and the risk managed in a way that is most suitable.

There are legal and statutory requirements for the protection of information, both personal and confidential, and this policy sets out how the risks to that information will be managed in compliance with those requirements.

4. Scope

This policy covers all organisational areas including information risk associated with third party provision of services.

5. Communication/Dissemination

This policy will be made available to all staff. The policy will be published, as a minimum, in the following ways:

1. Publication in the relevant policy section of the organisation's Internet
2. Publication in the Publication Scheme (Freedom of Information)

6. Definitions

A definition used in information risk management and this policy includes:

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 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.

Please refer to the Risk Management Policy for more definitions.

7. Duties and Responsibilities

7.1 Chief Officer

The Accountable Officer has overall responsibility for the organisation's risk management. Operational responsibility may be delegated to a Senior Information Risk Owner.

7.2 Senior Information Risk Owner

The SIRO will have lead responsibility for information risk and information risk management within the organisation. This position will be the Chief Finance Officer.

7.3 Data Protection Officer (DPO)

The DPO's role is to inform and advise the CCG and its staff about their obligations to comply with the General Data Protection Regulation (GDPR) and other data protection laws. This is a new role that the GDPR, which is set is replace the current Data Protection Act in May 2018, has brought in. The DPO will be required to monitor compliance with the GDPR and other data protection laws, including managing internal data protection activities, advise on data protection impact assessments; train staff and conduct internal audits. In addition they are required to be the first point of contact for supervisory authorities and for individuals whose data is processed (employees, customers etc.).

7.4 Audit Committee

This committee is responsible for the monitoring and assurances concerning information risk management. Operational responsibility is delegated to the Information Governance Operational Group, of which the SIRO and Caldicott Guardian are members.

7.5 Information Asset Owners

An Information Asset Owner (IAO) is responsible for the information managed within one or more information assets (system, process, files etc.). Part of the function of the IAO is to be aware of and manage local risks to information and where the risk is sufficiently high (see below) report the risk to their SIRO.

7.6 Information Risk Supporting Roles

In addition to the Information Asset Owners (IAO) and Information Asset Administrators (IAA) roles defined above, Information Risk supporting structure for the SIRO will consist of the CCG's Caldicott Guardian, Greater Manchester Shared Services (GMSS) IG Team and other appropriate Officers - agencies as required.

7.7 Staff

All staff will be aware of information risk management and understand the need for information risk to be a part of the culture of the organisation.

8. Policy Detail

The information risk management process will take place using the NHS "5x5 Risk Matrix" as detailed in the NPSA's "Risk Matrix for Risk Managers". This document contains guidance on how to interpret the scores that will be attributed to risks and provide the basis for information risk reporting to the Senior Management Team, Information on the matrix relating to this policy may be found in Appendix A and B.

8.1 Privacy Impact Assessments

Risks to personal and confidential information that arise as a consequence of changes to systems (projects) will be identified via the completion of a Privacy Impact Assessment (PIA). This will be a questionnaire completed by the project manager or other suitable project member who will be considered by IG and where necessary a report on information risks and actions to be taken will be produced. This will be managed as part of the overall project with IG oversight at all times. Privacy Impact Assessment processes and proformas are available from the GMSS IG Team or on the CCG's website.

8.2 Local Information Risks

It is the IAO's responsibility to be aware of, and formally record, information risks to the assets which they manage. Many risks will be managed and resolved locally, but higher risks will need to be managed via IG in order to ensure the organisation is aware of those risks and can be assured that active management of them is in place.

It is necessary to ensure a consistent approach to risk assessment and risk priority ratings so that all risks can be initially prioritised and ultimately agreed by the appropriate governance group. The board will be informed of significant risks. To ensure this consistency and assurance to each of the CCG Committees that the CCGs are managing their risks adequately and they use the following tools:

- Risk Management Process and Action Plans
- Risk Analysis and Recording
  - Risk Consequence Table
  - Risk Rating Matrix
  - Specific Risk Assessment Form
  - Risk Register Template

8.3 Management of Information Risks

An information asset is a body of information, defined and managed as a single unit so it can be understood, shared, protected and exploited effectively. Please refer to Appendix A and B for more information on Information Assets.

Information assets have recognisable and manageable value, risk, content and lifecycles. All breaches and incidents regarding Information asset should be reported directly to the CCG IG Lead and GMSS IG Officer.

Information risks will be managed locally, unless the risk score attributed to an individual risk is 15 or greater. The Risk Matrix and scoring is available for reference in the Risk Management Policy.

The treatment options for information risk are:

Avoid: not proceeding with activity likely to generate the risk

Reduce: reducing or controlling the likelihood and consequences of the occurrence

Transfer: arranging for another party to bear or share some part of the risk, through contracts, partnerships, joint ventures, etc.

Accept: some risks may be minimal and retention acceptable.

Risks will be managed via a standard risk log format that will enable risks managed consistently across organisations ensuring a high quality level of support, where it is necessary.

Information risks relating to sensitive personal data and confidential information in hard and soft format will be systematically evaluated throughout the IG team and the Risk Manager and action taken on a risk assessed basis.
All significant breaches will be included in the CCG's IG report.

All sensitive personal data will be handled as 'confidential information', kept securely in locked cabinets and via appropriate permissions on the network. It will be made available on a need-to-know basis and advice provided to staff as appropriate.

Policies are in place to support information risk management including information security, data protection, confidentiality and Record Management on the CCG's website.

All internal staff as well as third parties, contractors, agency staff will be required to sign and follow the CCG's Confidentiality clauses.

Privacy Impact Assessments will be carried out as necessary where new systems have the potential to negatively impact on personal privacy.

Escalation of Risks

Please refer to the CCG Risk Management Policy for more information on escalation of Risk.

The IAO will be responsible for managing the risks, reporting and ensuring that suitable mitigations are put in place either locally or with support from information governance/risk management.

The SIRO is responsible for ensuring that policy is followed and to be aware of all risks.

The Risk Register with terms of reference covering the management of risks will be responsible for organisational risk logs, where high risks are to be recorded. This group is also responsible for escalating high risks to the board and ensuring that where relevant they are admitted to the corporate risk register.

Proactive planning will be undertaken for investigating and identifying risks through different scenarios, regular policy reviews, ICO recommendations and assessment of sources of legal weight and admissibility of evidence for reducing risks.

8.4 Information Risk Management Training

NHS Digital provide a suite of IG training workbooks. Any member of staff that requires additional IG training for their job role will be directed to the relevant

workbook. The GMSS team have provided an IG Training Needs Analysis which provides further detail.

The IG training workbooks can be obtained by through the GMSS IG Team.

8.5 Information Asset Register

The CCGs will establish a programme to ensure that their Information Assets (IA's) are identified and assigned to an IAO. The SIRO will oversee a review of the organisation's asset register to ensure it is kept up to date, complete and robust.

All critical IA's will be identified and included within the Information Asset Register (IAR), together with details of business critical assets. The IAO and the Information Asset Administrator (IAA) will ensure that risk reviews are carried out. In order to improve the usability and maintainability, the Information Asset register may be organised by service, rather than by location. Refer to Appendix A and B for more information on Information Assets.

9. Support and Monitoring

Support will be provided to staff in assessing risk and managing their local processes by the IG and Risk teams, locally. Where necessary these teams will seek further advice on behalf of the department making the query.

Monitoring compliance with the policy will be done in the following ways:

- legislative changes; good practice guidance; case law;
- significant incidents reported; new vulnerabilities; and
- changes to organisational infrastructure.

10. References

- "Risk Matrix for Risk Managers" at **www.npsa.nhs.uk**.
- NHS Information Risk Management — NHS Digital
- Information Commissioner's Officer at **www.ico.org.uk**
- What security measures should I take to protect the personal data I hold? By ICO
- Notification of data security breaches to the Information Commissioner's Office by ICO

11. IG Related Documents

A set of procedural documents will be made available via GMSS Internet.

- Information Governance Framework
- Information Governance Policy

- Data Protection & Confidentiality Policy
- Information Governance & Cyber Incident Reporting Policy
- Secure Transfer of Information
- Records Management Policy
- Subject Access Procedure
- Information Governance Staff Handbook

This list is not exhaustive

Appendix A – Information Asset Information

Assessing whether something is an information asset

To assess whether something is an information asset, task the following questions:

- Does the information have a value to the CCG? How useful is it? Will it cost money to reacquire? Would there be legal, reputational or financial repercussions if you couldn't produce it on request? Would it have an effect on operational efficiency if this information could not be accessed easily? Would there be consequences of not having it?

- Is there a risk associated with the information? Is there a risk of losing it? A risk that it is not accurate? A risk that someone may try to tamper with it? A risk arising from inappropriate disclosure?

- Does the group of information have a specific content? Is there an understanding of what the information is and what it is for? Does it match the purpose associated with the information?

- Does the information have a manageable lifecycle? Were all the components created for a common purpose? Will they be disposed of in the same way and according to the same rules?

Examples of typical assets include:

Personal Information Content	**Software**
• Databases and data files • Back-up and archive data • Audit data • Paper records (patient case notes and staff records) • Paper reports	• Applications and System Software • Data encryption utilities • Development and Maintenance tools
Other Information Content	**Hardware**
• Databases and data files • Back-up and archive data • Audit data • Paper records and reports	• Computing hardware including PCs, • Laptops, PDA, communications devices e.g. blackberry and removable media
System/Process Documentation	**Miscellaneous**
• System information and • Documentation • Operations and support • Procedures • Manuals and training materials • Contracts and agreements • Business continuity plans	• Environmental services e.g. power and • air-conditioning • People skills and experience Shared service including Networks and • Printers • Computer rooms and equipment • Records libraries

Appendix B – Information Asset Risk Assessment Form

Information Asset Risk Assessment

Section 1: General Information

Asset Register No.:			
Information Asset / System Name:			
Description:			
Key Asset Status:			
Assessment Date:			
Undertaken By:			
Reviewed By:			
IAO:			
IAA:			
Composite Risk Score:	0	**Residual Risk Score:**	0
Risk Re-Review Period:			

Section 2: Information Risk Assessment

	Threats Areas	Composite Risk			Existing Controls	Gaps in Controls	Mitigation Action Plan	Target Date	Risk mitigated to acceptable level? Yes / No?	Target Risk		
		Likelihood	Impact	Score						Likelihood	Impact	Score
1	Unauthorised or inappropriate access											
2	Unauthorised or inappropriate use											
3	Introduction of damaging or disruptive software											
4	Failure of infrastructure											
5	Utilities and failure of environmental controls											
6	Network Failure											
7	Software Failure											
8	Maintenance / Support Error											
9	User Error											
10	Fire											
11	Flood											
12	Staffing and Resources											
13	Theft											
14	Wilful Damage											
15	Other Threat -please identify below:											