NHS

Bolton Clinical Commissioning Group

Information Risk Policy

Policy Number	**IG006**
Target Audience	**CCG/GMSS Staff**
Approving Committee	**CCG Chief Officer**
Date Approved	**December 2017**
Last Review Date	**December 2017**
Next Review Date	**December 2019**
Policy Author	**GMSS IG Team**
Version Number	**V4.0**

The CCG is committed to an environment that promotes equality, embraces diversity and respects human rights both within our workforce and in service delivery. This document should be implemented with due regard to this commitment.

This document can only be considered valid when viewed via the CCG's intranet. If this document is printed into hard copy or saved to another location, you must check that the version number on your copy matches that of the one online.

Approved documents are valid for use after their approval date and remain in force beyond any expiry of their review date until a new version is available.

Version Control Sheet

Version	Date	Reviewed By	Comment
0.1	September 2013	M Robinson D Sankey	Progress to CCG Executive for approval
1.0	September 2013	CCG Exec	Approved
1.1	June 2015	IG Team	Reviewed & progress to IM & T Operations Board for approval.
2.0	June 2015	IM & T Operations Board	Approval
3.0	June 2017	IG Team	Reviewed & progress to IM & T Operations Board for approval.
4.0	**December 2017**	**CCG Chief Officer**	**Approved.**

Analysis of Effect completed:	By: M Robinson	Date: September 2013

Contents

1. Introduction, Purpose and Scope

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

1.2 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.

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

1.4 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 Framework as well as the Information Governance Policy, Data Protection and Confidentiality Policy and Record Management Policy.

1.5 **Purpose -** The purpose of this policy is to provide a consistent way of managing information risk in the CCG, 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 CCG. 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.

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

2. Communication / Dissemination

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

- Publication in the relevant policy section of the CCG’s Internet and Intranet;
- Emailed to staff via the Staff Bulletin;
- Line manager;
- Team meetings;
- Specific training course.

3. Definitions

3.1 Definitions used in this Policy and risk management include:

- **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 as 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.
- **Treatmen**t: 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.

3.2 Please refer to the CCG's Risk Management Strategy for more definitions.

4. Accountability, Responsibilities and Training

4.1 The Chief Officer has ultimate responsibility for the implementation of the provisions of this policy. As the 'Accountable Officer' they are responsible for the management of the CCG and for ensuring that the appropriate mechanisms are in place to support service delivery and continuity.

4.2 The Senior Information Risk Owner has overall responsibility for information risk and information risk management within the CCG. This position will be a director level role.

4.3 Committees:

- Bolton CCG Board - hold ultimate responsibility for identifying and authorising management actions and access to appropriate resources to mitigate High risks;
- The Audit Committee - provides the CCG Board with assurance that risk management systems are working and that adequate controls are in place for all significant risks. The Audit Committee will receive details of risks identified as Significant 12 or above at least twice a year and details of the controls in place to mitigate against those risks;
- The CCG Executive Team - is a Committee of the CCG Board and will routinely monitor the management of all risks placed on the Risk Register and provide opinion regarding acceptable risk and residual

risk. The CCG Executive Team will receive assurance on all aspects of risk management and is responsible for ensuring that CCG Board / Audit Committee are fully informed of all significant threats to the CCG and its objectives. They will ensure where necessary, a risk is escalated to the CCG Board via its regular reporting mechanisms. In addition they will routinely review progress on the annual priorities of the CCG and identify risks and areas of concern to the CCG, identify and implement solutions.

- Quality & Safety Committee - reports direct to the CCG Board and is responsible for reviewing Quality / Performance risks relating to the quality of NHS care commissioned by the CCG. It will review and update appropriate risks contained in the Risk Register. This information will be reported to the CCG Executive Team as part of the CCG Executive Team's routine review of the Risk Register.
- Other management, project groups or sub committees of CCG (for example the IM&T Operations) - is required to identify and monitor risks in their respective area and to report risks as appropriate for inclusion in the Risk Register.

4.4 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.

4.5 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

4.6 Line managers will take responsibility for ensuring that the Information Risk Policy is implemented within their group or directorate.

4.7 It is the responsibility of each employee to adhere to the policy and be aware of information risk management and understand the need for information risk to be a part of the culture of the CCG.

4.6.1 All staff are mandated to undertake the “Introduction to Information Governance,” the GMSS IG Team will direct staff to the current module. Information Governance training is required to be undertaken on an annual basis.

5. Policy Detail

5.1 The information risk management process will take place using the CCG “5x5 Risk Matrix” (Appendix A). Staff / Managers should complete the CCG's Assessment form (Appendix B) which should then be submitted to the

Governance and Risk Department and included on the CCG Risk Register as necessary.

5.2 **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, Information Asset Owner or other suitable project member that will be considered by Information Governance Leads 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 information governance oversight at all times.

CCG Privacy Impact Assessment Process IG011 provides further details.

5.3 **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 IM&T Operations Board to ensure the CCG is aware of those risks and can be assured that active management of them is in place.

5.3.1 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 risks are being managed adequately 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

5.4 **Management of 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 C for more information on Information Assets

5.4.1 Information assets have recognisable and manageable value, risk, content and lifecycles. All breaches and incidents regarding Information asset should be reported using CCG's online incident reporting system – Safeguard

.

5.4.2 Information risks will be managed locally, unless the risk score attributed to an individual risk is 12 or greater. The Risk Matrix and scoring is available for reference in the CCG's Risk Management Strategy (RMS).

5.4.3 The treatment options for information risk are:

- **Avoid:** not proceeding with activity likely to generate the risk
- **Reduce**: reducing or controlling the likelihood of 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

5.4.4 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.

5.4.5 Information risks relating to sensitive personal data and confidential information in hard and soft format will be systematically evaluated throughout the Information Governance team and the Governance, Risk and Complaints Manager and action taken on a risk assessed basis. All significant breaches will be reviewed / investigated as per the Information Governance Incident Reporting Procedure.

5.4.6 Policies are in place to support information risk management including Corporate Information Security, Confidentiality and Data Protection, and Record Management on the CCG's internet.

5.5 **Escalation of Risks** - If any individual threat obtains a risk score greater than 12, these will be reported to the Governance, Risk and Complaints Manager and follow the escalation process as per the CCG's Risk Management Strategy. These risks will also be reviewed at the IM&T Operations Board with actions / recommendations assigned where applicable.

5.5.1 Risks of 12 or higher will be reported to the SIRO, and included in the Board Assurance Framework which is reported to the CCG Executive Team, Audit Committee and the CCG Board.

5.5.2 The CCG Executive Team 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.

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

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

5.6 **Information Risk Management Training** - Any personnel involved in information risk management must complete the required training. Those with the assigned roles of SIRO, Information Asset Owners (IAO's) and Information Asset Administrators (IAA's) must complete the training annually and others when necessary will be asked to complete.

5.6.1 Training compliance can be achieved by either:

a) Attendance at an external information risk course such as IAO Training;

b) Completion of the identified modules via online systems – contact the GMSS IG Team for information on how to access these modules.

5.7 **Information Asset Register** – The CCG have an established programme to ensure that their Information Assets (IA's) are identified and assigned to an IAO. The SIRO will oversee a review of the CCG's asset register to ensure it is kept up to date, complete and robust.

5.7.1 All critical IA's are identified and included within the Information Asset Register (IAR), together with details of business criticality, the IAO, the Information Asset Administrator (IAA) and risk reviews to be 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 C for more information on Information Assets.

5.8 **Data Flow Mapping -** For any assets that process information either inbound from or outbound to external organisations it will be necessary to complete a data flow mapping register (DFM). These are normally reserved for Personal Confidential Data (PCD) however to ensure there is visibility of other business sensitive / confidential data, these flows are to be mapped as well.

5.8.1 The DFM Register will hold the information about each flow, contact details, method of transfer and what controls are in place to ensure that information is kept secure.

5.8.2 IAO's are required to check the register at least annually or when any new / changed data flow occurs to ensure the register is up to date.

5.8.3 The IG Team undertake regular checks on the data flow mapping register and risk assess each flow to ensure this is at an acceptable level and / or recommend actions when necessary to improve safeguarding of information.

6. Support and Monitoring

6.1 Support will be provided to staff in assessing risk and managing their local processes by the Information Governance Leads and the Governance and Risk Department. Where necessary these teams will seek further advice on behalf of the department making the query.

6.2 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.

6.3 This policy will be monitored through staff awareness and supporting evidence to the NHS IG Toolkit.

7. Other Relevant Procedural Documents

IG001 Information Governance Policy
IG002 Confidentiality and Data Protection Policy
IG003 Corporate Information Security Policy
IG004 Acceptable Use Policy (IT, Email and Internet)
IG005 Records Management Policy
IG007 Information Governance Incident Reporting Procedure
IG008 Encryption Policy
IG009 Confidentiality Audit Procedure
IG011 Privacy Impact Assessment Process

This list is not exhaustive

8. 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

Appendix A - Bolton CCG Risk Assessment Tool and Grading Matrix

1. Table 1 Consequence scores (I)

Choose the most appropriate domain for the identified risk from the left hand side of the table Then work along the columns in same row to assess the severity of the risk on the scale of 1 to 5 to determine the consequence score, which is the number given at the top of the column.

Grade	1	2	3	4	5
Category	**Very Low**	**Minor**	**Moderate**	**High**	**Severe**
People and Change **(Human resources/ organisational development/staffing/ competence)**	Short-term low staffing level that temporarily reduces service quality (< 1 day)	Low staffing level that reduces the service quality	Late delivery of key objective/ service due to lack of staff Unsafe staffing level or competence (>1 day) Low staff morale Poor staff attendance for mandatory training	Uncertain delivery of key objectives due to lack of staff Unsafe staffing level (>5 days) Loss of key staff Very low staff morale No staff attending mandatory/ key training	Non-delivery of key objective/ service due to lack of staff Ongoing unsafe staffing levels or competence Loss of several key staff No staff attending mandatory training /key training on an ongoing basis
Strategic **(Business objectives/ projects)**	Insignificant cost increase/ schedule slippage	<5 per cent over project budget Schedule slippage	5–10 per cent over project budget Schedule slippage	Non-compliance with national 10–25 per cent over project budget Schedule slippage Key objectives not met	Incident leading >25 per cent over project budget Schedule slippage Key objectives not met
Clinical Quality - Patient Safety	No medical attention required. No impact beyond 1 day.	Single person requiring medical attention but not hospital admission, multiple minor incidents.	Single hospital admission, multiple minor injuries requiring medical attention.	Single fatality or permanent disability; or multiple injuries requiring hospital admission.	Multiple fatalities or permanent disabilities.
Clinical Quality – Clinical Effectiveness	Minor breach of guidance – no impact on patient outcomes.	Significant breach leading to harm for a small number of patients.	Significant breach of guidance leading to harm for a number of patients.	Breach leading to reduced life expectancy for multiple people.	Multiple fatalities or permanent disabilities.
Clinical Quality – Patient Experience	Minor inconvenience to single individual.	Minor inconvenience to many individuals, significant inconvenience to single individual.	Significant inconvenience to many individuals, patient experience impact on health outcomes for a few.	Patient experience impact on health outcomes for a significant number.	Multiple fatalities or permanent disabilities.
Health Inequalities	Possible increase to inequalities.	Probable small increase to inequalities.	Probable significant increase to inequalities.	Actual small increase to inequalities.	Actual substantial increase to inequalities.
Health Improvement	Possible slowing of decline of prevalence.	Probable slight slowing in rate of improvement in death rates, No decline or	Probable significant slowing in improvement of death rates.	Slight increase in death rates. Substantial increase in prevalence.	Substantial increase in death rates.

		significant slowing in prevalence.	Slight increase in prevalence.		
Health Protection	Minor injury or illness requiring no medical attention.	Injury or illness requiring medical attention for a few.	Injury or illness requiring a few hospital admissions, or multiple numbers requiring medical attention.	Single fatality or permanent disability; or multiple injuries requiring hospital admission.	Multiple Fatalities.
Operational **and** **Legal Compliance**	Minor breach of standards with no impact on organisation.	Breach of broader health standards or minor targets.	Breach leading to discussion with NCB.	Breach leading to DH improvement team intervention. Breach leading to threat of court action.	Breach leading to court action against executive.
Financial Balance	<£1,000 loss.	£1,000 - £25,000 loss.	£25,001 - £250,000 loss.	£250,001 - £2,000,000 loss.	>£2million loss.
Financial Governance	Isolated technical breach with minimal impact.	Numerous minor technical breaches. Technical breach leading to financial loss.	Limited assurance on single key financial systems.	Failure to get Statement on Internal Control agreed. Fraud leading to imprisonment of staff member. No assurance on single key financial system. Limited assurance on multiple systems.	Fraud >£2million. Investigation by the Audit Commission. No assurance on multiple financial systems.
Information and Technology **(Information Governance)**	Minor technical breaches of standards not directly impacting on members of the public.	Single loss of data or other breach affecting a single individual.	Multiple losses of data or other breaches of governance standards impacting on small numbers of people. Single loss of data impacting on many people.	Multiple losses of data or other breaches of governance standards each impacting on hundreds of individuals.	Breach leading to court action against executive.
Staff Safety and Wellbeing	Minor cuts and bruises. Isolated incidence of low morale	Medical treatment required. Less than three days' absence. Low morale among a number of staff groups.	Single admittance to hospital for less than 24 hours. Absence of three days or longer. Sickness rates increasing.	Single fatality or permanent disability. Rapid increase in sickness rates threatening service delivery	Multiple fatalities or cases of permanent disability.
Governance and reputation	Complaint /concern only	Failure to follow agreed procedures. Minor out of court settlement. Two days or less coverage in local press.	Inappropriate decision making. Local press coverage longer than two days. Two days or less of national media coverage	National media coverage longer than two days. NCB/DoH intervention. Questions in the House. Class action, Criminal prosecution.	Imprisonment of executive officer. Full public enquiry.

2. Table 2 Likelihood score (L)

What is the likelihood of the consequence occurring?

The frequency-based score is appropriate in most circumstances and is easier to identify. It should be used whenever it is possible to identify a frequency.

Likelihood score	**1**	**2**	**3**	**4**	**5**
Descriptor	**Rare**	**Unlikely**	**Possible**	**Likely**	**Almost certain**
Frequency How often might it/does it happen	This will probably never happen/recur Not expected to occur for years	Do not expect it to happen/recur but it is possible it may do so Expected to occur annually	Might happen or recur occasionally	Will probably happen/recur but it is not a persisting issue	Will undoubtedly happen/recur,possibly frequently

3. Overall Risk Grading/Score (R)

	IMPACT / CONSEQUENCE					
LIKELIHOOD		**1**	**2**	**3**	**4**	**5**
	1	**Low 1**	**Low 2**	**Low 3**	**Moderate 4**	**Moderate 5**
	2	**Low 2**	**Moderate 4**	**Moderate 6**	**Significant 8**	**Significant 10**
	3	**Low 3**	**Moderate 6**	**Significant 9**	**Significant 12**	**High 15**
	4	**Moderate 4**	**Significant 8**	**Significant 12**	**High 16**	**High 20**
	5	**Moderate 5**	**Significant 10**	**High 15**	**High 20**	**High 25**

Overall risk key

1-3	Low risk
4-6	Moderate risk
8-12	Significant risk
15-25	High risk

Risk Assessment

1 Define the risk(s) explicitly in terms of the adverse impact or consequence (I) that might arise.

2 Use Table 1 to determine the consequence score(s) for the potential adverse outcome(s) relevant to the risk being evaluated.

3 Use Table 2 to determine the likelihood score(s) (L) for those adverse outcomes. If possible, score the likelihood by assigning a predicted frequency of occurrence of the adverse outcome. If this is not possible, assign a probability to the adverse outcome occurring within a given time frame, such as the lifetime of a project or a patient care episode. If it is not possible to determine a numerical probability then use the probability descriptions to determine the most appropriate score.

4 Calculate the risk score the risk multiplying the consequence by the likelihood: I (impact) x L (likelihood) = R (risk grading/score)

5 Identify the level at which the risk will be managed in the organisation, assign priorities for remedial action, and determine whether risks are to be accepted on the basis of the colour bandings / risk rating, and the organisation’s risk management system. Include the risk in the organisation’s Risk Register.

Appendix B – Risk Assessment Form (Risk Identification, Evaluation and Risk Reduction Action Plan)

1: Identify the Risk/s

Firstly you need to detail the potential risk/s? Identify what, where, when, why and how events could prevent, delay or degrade the achievement of the intended action/outcome.

2: Analyse the Risk/s

Identify and evaluate existing controls. Determine the consequence and likelihood and hence the risk rating. This analysis should consider the potential consequences and how these could occur.

3: Evaluate the Risk/s

(How bad and how often) and decide on the existing precautions (controls) and decide if there is a need for further precautions (controls)? Consider the balance between potential benefits and adverse outcomes. This will enable decisions to be made in respect of the extent and nature of actions required and about priorities.

List the existing controls

List any additional controls that may be required

RISK RATING TAKING INTO ACCOUNT THE EXISTING CONTROLS ONLY:

Likelihood level		**x**	**Impact level**		**=**	

<table>
<tr><th colspan="2">Risk Assessment No</th><th colspan="3">ACTION/s
(Additional control measures required to reduce the risk to the lowest possible level)</th><th>Designated Lead
(Action by)</th><th>Review Date</th><th>Deadline</th></tr>
<tr><td colspan="2"></td><td colspan="3"></td><td></td><td></td><td></td></tr>
<tr><td colspan="2"></td><td colspan="3"></td><td></td><td></td><td></td></tr>
<tr><td colspan="2"></td><td colspan="3"></td><td></td><td></td><td></td></tr>
<tr><td colspan="2"></td><td colspan="3"></td><td></td><td></td><td></td></tr>
<tr><td colspan="2"></td><td colspan="3"></td><td></td><td></td><td></td></tr>
<tr><td colspan="2"></td><td colspan="3"></td><td></td><td></td><td></td></tr>
<tr><td colspan="8"><b>RESIDUAL RISK RATING AFTER ADDITIONAL CONTROLS HAVE BEEN IMPLEMENTED:</b></td></tr>
<tr><td>Likelihood level</td><td></td><td>x</td><td>Impact level</td><td></td><td>=</td><td colspan="2"></td></tr>
</table>

<table>
<tr><th colspan="5">5: MONITOR AND REVIEW</th></tr>
<tr><th>Date of review</th><th>Reviewer/s</th><th>Findings</th><th>Revised Risk Score</th><th>Corporate/Directorate Risk Register – Date Revised</th></tr>
<tr><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td><td></td></tr>
</table>

Appendix C - Information Asset

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. 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 D – Risk Assessment Template

IAR Risk Assessment Template