Bolton
Clinical Commissioning Group

Information Risk Policy

Policy Number	**IG006**
Target Audience	**CCG Staff**
Approving Committee	**CCG Chief Officer**
Date Approved	**July 2019**
Last Review Date	**June 2019**
Next Review Date	**June 2021**
Policy Author	**IG Team**
Version Number	**V5.1**

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.
4.1	June 2019	IG Team	Reviewed & updated in line with GDPR & DPA 2018
5.0	June 2019	IG Board	Approved
5.1	July 2019	CCG Chief Officer	Approved

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

Contents

1. Introduction

Information risk management is an essential element of broader information assurance and is an integral part of good management practice. The intent is to embed information risk management in a very practical way into Bolton Clinical Commissioning Group's (here after referred to "the CCG") business processes and functions. This is achieved through key approval and review processes / controls – and not to impose risk management as an extra requirement.

Information is a vital asset, both in terms of the management of health and social care for individual patients / service users and the efficient management of services and resources. It plays a key part in governance, service planning and performance management.

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

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

Information risk must be managed in a robust way within work areas and not be seen as something that is the sole responsibility of IT or IG staff. A structured approach is needed, building upon the existing CCG's IG framework and this approach relies upon the identification of information assets and assigning 'ownership' of assets to senior accountable staff.

It is therefore of paramount importance to ensure that information is efficiently managed including information risk, and that appropriate policies, procedures and management accountability provide a robust governance framework for information management.

2. Purpose and Scope

This policy ensures that all managers and staff are aware of and comply with the CCG's statutory obligations and responsibilities regarding information risk, including those under the Data Protection Act (DPA), and the General Data Protection Regulations (GDPR).

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.

This policy aims to encourage pro-active information risk management, in order to provide assistance and improve the quality of decision-making throughout the CCG, and help to safeguard the CCG's information assets.

This policy outlines the requirements of 'data protection by design' to ensure that privacy and data protection is a key consideration in the early stages of any project, and then throughout its lifecycle, and also to ensure that processes for completing and reviewing Data Protection Impact Assessment and where applicable System Level Security Procedure are managed in a consistent and controlled way.

The CCG have a legal obligation to comply with appropriate legislation ensuring 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.

3. Legislations, Regulations and Guidance

General Data Protection Regulation 2016 and the Data Protection Act 2018

The General Data Protection Regulation (GDPR) became applicable in UK law from 25th May 2018 coinciding with the UK Data Protection Act (DPA) 2018. The GDPR applies to Data Controllers and Data Processors who process personal and / or special category of data. The GDPR replaced the 1995 data protection directive which originated the DPA. The DPA 2018 sits along with the GDPR governing how we collect, store, process and share data in the UK. It fills in the gaps where flexibility and derogations are permitted in the UK and will ensure that the provisions in the GDPR will be applicable in the UK post Brexit. This policy has been revised to reflect the CCG's obligations under the GDPR and DPA.

The principles of this data protection legislation specify that appropriate technical and organisational measures must be in place to secure against unauthorised or unlawful processing of information, and to protect information from accidental loss, destruction or damage. In practice, this means that the CCG must ensure that:

- Security measures are designed and organised to fit the nature of the information being held and the level of harm that may result from a breach;
- Staff are clear about their responsibilities relating to information risk and security, as well as those of the Senior Information Risk Owner (SIRO), Information Asset Owners (IAOs) and Managers (IAMs);
- Appropriate physical and technical security is in place for all information, backed up by robust policies and procedures, and reliable, knowledgeable and well-trained staff;
- Breaches can be dealt with swiftly, effectively and consistently;
- There are other rules and regulations which specify how information should be handled. These include, but are not limited to:
    - Access to Health Records 1990
    - Code of Practice on Confidential Information 2014
    - Common Law Duty of Confidentiality
    - Computer Misuse Act 1990
    - Confidentiality NHS Code of Practice
    - Crime and Disorder Act 1998
    - Criminal Justice and Immigration Act 2008

- Freedom of Information Act 2000
- HSCIC Guide to Confidentiality 2013
- Human Rights Act 1998 (Article 8)
- Records Management Code of Practice 2016

The GDPR introduces a new obligation to undertake a Data Protection Impact Assessment (DPIA) before carrying out types of processing likely to result in high risk to individuals' rights and freedoms. This is a key part focussing on accountability and 'data protection by design.' This will assist the CCG in understanding whether appropriate technical and organisational measures are in place to safeguard information at all stages.

Failure to meet the requirements of this policy, which reflect the CCG's obligations under data protection legislation, exposes the organisation to enforcement action and fines. Allowing the Information Commissioner to levy higher administrative fines on data controllers and processors for the most serious data breaches, which may be up to £17m (€20m) or 4% of global turnover.

4. Definitions

Definitions used in this Policy and Risk Management include:

Information Assets:
The following are examples of information assets:

- Databases and data files
- System information and documentation
- Operations and support procedures
- Audit data
- Manuals and training materials
- Contracts and agreements
- Business continuity plans
- Back-up and archive data
- Applications and System Software
- People skills and experience
- Shared services, including networks and printers
- Paper records, including patient case notes and staff records.

For more information on information assets refer to Appendix C.

Personal Data:
Personal data means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person

Special Categories of Personal Data:
Special Category Data is personal data which the GDPR says is more sensitive, and so needs more protection. These special categories of data are:

- Racial or ethnic origin;
- Political opinions;
- Religious or philosophical beliefs;
- Trade Union membership;
- Health Data;
- Sexual life / sexual orientation;
- Genetic data – introduced under GDPR;
- Biometric data – introduced under GDPR.

Processing:
Processing means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Data Controller:
This means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

Data Processor:
This means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

Risk Terminology:

Key Terms	Description
Breach	Any event or circumstance that led to unintended or unexpected harm, loss or damage.
Near-Miss	Any event or circumstance which was avoided but had the potential to lead to unintended or unexpected harm, loss or damage.
Serious Incidents Requiring Investigation (SIRI)	Any breaches where the consequences are so significant or the potential for learning is so great that a heightened level of response is required.
Risk	The chance of something happening or a hazard being realised, which will have an impact on objectives. This may be damage to information or reputation or may involve injury or liability. 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 measure of the probability that the consequence will occur, as a qualitative description or synonym.
Risk Management	The systematic application of management policies, procedures and practices to the tasks of identifying, analysing, assessing, treating and monitoring risk.
Risk Assessment	The overall systematic process of determining the level of risk that an event/set of events poses in combination with the likelihood of its occurrence.
Risk Rating	The 'score' that a risk is given following risk assessment using a risk matrix.
Control	An activity (action) which reduces the consequence and/or likelihood
Risk Mitigation	The process of introducing specific measures (controls) to minimise or eliminate risks. Risk mitigation measures can be directed towards reducing the severity of risk consequences, reducing the likelihood of the risk occurring, or reducing the organisations exposure to the risk.

Further definitions are available in the CCG's Risk Management Strategy.

5. Accountability and Responsibilities

Chief Officer
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.

Senior Information Risk Owner
The Senior Information Risk Owner (SIRO has overall responsibility for information risk and information risk management within the CCG. This position will be a director level role. The current SIRO is the CCG's Chief Finance Officer.

The SIRO advises the Board on the effectiveness of information risk management across the CCG. The SIRO is responsible for:

- ensuring that information assets are identified, that a register of assets is maintained, and that each major asset has an assigned owner and administrator;
- coordinating and overseeing the development and implementation of the Information Risk Policy;
- ensuring that systems, policies, processes and standards are in place to ensure rigorous information governance across the CCG;
- ensuring that the CCG Board is adequately briefed, and providing a focal point for the resolution and discussion of information risk issues, advising on information security and risk management strategies and providing periodic reports and briefings on progress

Information Asset Owner
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.

An IAO is a nominated manager/senior member of staff who takes responsibility for individual information assets, in terms of security, user access, risk assessment and business continuity. They are supported by an Information Asset Manager (IAM) and Information Asset Administrator (IAA), per asset (this can be the same person).

Within the CCG, IAOs are usually Associate Directors or Heads of Department however the level of authority required for an asset will depend on the type of asset and the information it contains.

The responsibilities of an IAO are outlined below:

- ensuring that all information assets are appropriately owned, managed and recorded on the Information Asset Register (IAR);
- supporting the Senior Information Risk Owner (SIRO) in managing the risks associated with all information assets, and providing the SIRO with reports and risk assessments as required;
- ensuring that the Data Protection By Design Compliance Checklist is completed;
- ensuring that a Data Protection Impact Assessment (DPIA) is completed for all new and amended information assets, and this is regularly reviewed;
- ensuring that a System Level Security Procedure (SLSP) is completed for all new and amended systems, and this is regularly reviewed;
- ensuring that business continuity strategies and plans are in place and tested for all critical information assets.

Information Asset Managers
An Information Asset Manager (IAM) is a nominated administration, clerical or operational member of staff who takes responsibility for individual information assets, in terms of security, user access, risk assessment and business continuity. They support allocated IAOs with information assets.

Within the CCG, IAMs are usually senior administration or senior operational staff, however the level of authority required for an asset will depend on the type of asset, the information that it contains and the authority level of the IAO.

IAMs are responsible for supporting the relevant IAO(s) with meeting their responsibilities.

Information Asset Administrators
An Information Asset Administrators (IAAs) is classed as any member of staff who may use any of assets that relate to their work on a regularly basis

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

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.

All Staff
Every member of staff is personally responsible for taking precautions to ensure the security of information, both whilst it is in their possession and when it is being transferred from one person or organisation to another. If staff are unsure about sharing information they should take advice from their line manager or the IG Team, as appropriate.

Staff who manage or lead on projects / service changes are also responsible for assisting IAOs completing a Data Protection by Design Compliance Checklist, Data Protection Impact Assessments (DPIA) and if applicable a System Level Security Procedure (SLSP). Additional responsibilities apply to Information Asset Owners (IAOs – see above) and Information Asset Managers (IAMs – see above).

To ensure that staff are effectively informed about what is required of them in relation to information risk and security, this policy has been produced to identify the legal requirements and provide an understanding of what the CCG requires staff to do to keep personal data safe and secure.

Failure to comply with data protection legislation can lead to enforcement action from the ICO, including monetary penalty notices, claims for compensation and / or criminal prosecution. It is the responsibility of every individual member of staff to be familiar with this policy (and all other related policies) to ensure the confidentiality, security and integrity of information is maintained whilst under their ownership. Any failure by a member of staff to follow the processes outlined in this policy may result in initiation of the CCG's Staff Disciplinary Procedure.

In addition, all staff are mandated to undertake the Data Security Awareness module which is the Information Governance training, and must be completed on an annual basis.

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 IG Board) - is required to identify and monitor risks in their respective area and to report risks as appropriate for inclusion in the Risk Register.

6. Assessment & Management of Information Risks

Assessment:
The CCG will assess information risk in a number of ways, which will include the following;

The organisation's risk management procedures provide clear guidance as to the way in which risks and incidents are identified, assessed and managed across the organisation, and how the information risks supports this process. Investigating and learning from incidents will support the organisation in understanding the real level of risk being experienced and in adjusting the controls in place.

Routine review of what information assets the CCG holds ensuring they have identified Information Asset Owners and that they are appropriate, known as the CCG's Information Asset Register.

Routine review of flows of personal data to ensure any risks identified with these flows are mitigated, including ensuring appropriate controls are in place for data transferred outside the EEA, known as the CCG's Data Flow Mapping Register.

Adopting a Data Protection by Design approach, undertaking Data Protection Impact Assessments and where applicable System Security Level risk assessments as methods through which information assets can be risk assessed and assured it complies with the required standards

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.

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 Information Asset Register (IAR) to ensure it is kept up to date, complete and robust.

The CCG's information assets are recorded on a central Information Asset Register (IAR), which is maintained by the IG Team. The IAR helps managers and the CCG to identify who is responsible for what assets (IAOs).

All critical IA's are identified and included within the IAR, together with details of business criticality, the IAO, the Information Asset Manager (IAM) and risk reviews to be carried out. In line with GDPR where personal data is contained within an asset there is a legal basis detailing why this information can be held. In order to improve the usability and maintainability, the IAR may be organised by service, rather than by location. Refer to Appendix C for more information on Information Assets.

The IAR is populated, updated and maintained using information provided by IAOs and Managers via the CCG's IG Team and where applicable the CCG's Data Protection Impact Assessment (DPIA) process. Reviews of IARs are carried out on an annual basis or where new information assets are identified.

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 data however to ensure there is visibility of other business sensitive / confidential data, these flows are to be mapped as well.

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.

The CCG cannot control how they receive information from external organisations (inbound flow), although guidance should be given where personal data is being received. Where information needs to be transferred out of the CCG it is important,

particularly where personal / confidential data is concerned, that this is done in a secure manner. For further advice contact the IG Team on methods of transfer.

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.

The IG Team undertake regular checks on the DFM 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.

Data Protection by Design - 'Data Protection by Design' is an approach to projects that promotes privacy and data protection compliance from the start. This approach is a requirement of data protection legislation and therefore the CCG must ensure that privacy and data protection is a key consideration in the early stages of any project, and then throughout its entire lifecycle.

Data Protection by Design is not just the completion of a Data Protection Impact Assessment it involves all the measures that can be taken to ensure that data is protected, secure and confidential from when the idea of using personal data is originally thought about.

Privacy considerations should be integrated into existing project management and risk management methodologies and policies.

Taking a 'Data Protection by Design' approach is an essential tool in minimising privacy risks and building trust. Designing projects, processes, products or systems with privacy in mind at the outset can lead to benefits which include:

- Potential problems are identified at an early stage, when addressing them will often be simpler and less costly;
- The CCG is more likely to meet its legal obligations and avoid breaches of the GDPR and DPA;
- Actions are less likely to be privacy intrusive and have a negative impact on individuals;
- Increased awareness of privacy and data protection across the CCG.

For more information please refer to the CCG's Data Protection by Design Checklist.

Data Protection Impact Assessments (DPIA) - Risks to personal and confidential information that arise as a consequence of changes to systems / processes (projects) will be identified via the completion of a DPIA. DPIAs are an integral part of a 'Data Protection by Design' approach and is the tool, a questionnaire, that the CCG uses to identify, and where possible reduce, the IG risks of projects, processes and systems within the organisation.

GDPR dictates that a DPIAs are mandatory where the data processing is "likely to result in a high risk to the rights and freedoms" of the data subject(s). This is particularly relevant where there is any automated processing (including profiling) or where the processing involves any special categories of data (such as health or social care information). The ICO has published information on completion of DPIAs on their website:

https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/

The CCG takes the approach that a DPIA should be completed whenever a new or updated system / process is proposed, processing personal data, which will or could potentially introduce new (or make changes to the existing) data management processes.

DPIAs must be completed by the project manager, IAO and / or other suitable project member that will be considered by the IG team 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.

DPIAs will be reviewed and approved by the IG Board. Information assets arising from DPIA will be updated on the relevant departments IAR where it will be noted that a DPIA was completed and approved.

Refer to the CCG's Data Protection Impact Assessment Procedure and Proforma (IG011) for further details.

System Level Security Procedure - The development, implementation and management of a System Level Security Procedure (SLSP) will help to demonstrate understanding of IG risks and commitment to address the security and confidentiality needs of a particular system.

"System" relates to the complete data handling solution (electronic or otherwise) of personal data / special category data.

An effective SLSP will therefore contain a considered and specific view of the range of security policy and management issues relevant to a system and that may encompass a range of technical, operational and procedural security topics.

The SLSP must be completed by the project manager, IAO, IT Leads and will be considered by IG and IT leads.

Refer to the CCG's System Level Security Procedure (IG017) for further details.

Management:

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 Board to ensure the CCG 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 SIRO will be informed of significant risks and if necessary inform the CCG Board

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

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

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, more information on how to report can be found within the Data Security & Protection Breaches / Incident Reporting Policy and Procedure.
.
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).

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

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 special category data and confidential information in hard and soft format will be systematically evaluated throughout the IG team and the Governance team and action taken on a risk assessed basis. All significant breaches will be reviewed / investigated as per the Data Security & Protection Breaches / Incident Reporting Policy and Procedure.

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.

Escalation of Risks - If any individual threat obtains a risk score greater than 12, these will be reported to the Governance team and follow the escalation process as

per the CCG's Risk Management Strategy. These risks will also be reviewed at the IG Operations Board with actions / recommendations assigned where applicable.

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.

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.

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.

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

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 Managers (IAM's) must complete the training annually and others when necessary will be asked to complete.

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 IG Team for information on how to access these modules.

7. Support and Monitoring

Support will be provided to staff in assessing risk and managing their local processes by the IG team and the Governance and Risk Department. 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.

This policy will be monitored through staff awareness and supporting evidence to the CCG's IG agenda.

8. Other Relevant Procedural Documents

RM001 Risk Management Strategy
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 Data Security & Protection Breaches / Incident Reporting Policy and Procedure
IG009 Confidentiality Audit Procedure
IG011 Data Protection Impact Assessment Procedure and Proforma
IG017 System Level Security Procedure

This list is not exhaustive

9. References

Risk Matrix for Risk Managers - www.npsa.nhs.uk.
NHS Information Risk Management — NHS Digital
Information Commissioner's Officer - www.ico.org.uk

Appendix A - Bolton CCG Risk Assessment Tool and Grading Matrix

1. Table 1 Impact 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. Based on

Grade Category	1 Very Low	2 Minor	3 Moderate	4 High	5 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 significant	Probable significant slowing in improvement of death rates. Slight increase in	Slight increase in death rates. Substantial increase in prevalence.	Substantial increase in death rates.

		slowing in prevalence.	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 impact/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/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**		**=**	**DATE**

Risk Assessment No	ACTION/s *(Additional control measures required to reduce the risk to the lowest possible level)*	Designated Lead *(Action by)*	Review Date	Deadline

RESIDUAL RISK RATING AFTER ADDITIONAL CONTROLS HAVE BEEN IMPLEMENTED:						
Likelihood level		**x**	**Impact level**		**=**	

5: MONITOR AND REVIEW				
Date of review	**Reviewer/s**	**Findings**	**Revised Risk Score**	**Risk Register Reference – Date Revised**

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