

Information Risk Policy

To be read with:

- Incident Reporting and Management Policy
- Information Governance Policy
- Serious & Untoward Incident Policy
- Risk Management Policy and Strategy
- Information Security Policy

Other Relevant Documentation:

- Information Asset Register

Version	1.1
Status	Ratified
Author/Lead	Information Governance & Data Protection Officer
Directorate	Finance and Performance
Ratified By	ICT & Information Governance Programme Group
Date Ratified	12 October 2010
Date Issued	12 October 2010
Date of Next Formal Review	24 February 2011
Target Audience	All Staff

“The PCT incorporates and support the human rights of the individual as set out in the European Convention on Human Rights and the Human Rights Act 1998”

Version Control Record

Version	Description of Change(s)	Reason for Change	Author	Date
0.1	Initial Draft		Information Governance and Data Protection Officer	25/08/2009
0.2	Reference made to Information Security Officer	IG Toolkit requirements	Information Governance and Data Protection Officer	27/08/2009
0.3	Reference made to identify both Brent Community Services and NHS Brent SIROs	Comments from Director of Finance & Performance	Information Governance and Data Protection Officer	07/10/2009
0.4	BCS Head of Governance added to section 4.1, and Appendix 4 updated to new format.	Comments from Head of Corporate Affairs	Information Governance and Data Protection Officer	08/10/2009
0.5	Amendments to Information Security Officer and Information Asset Owners.	Comments from Director of Finance & Performance and Deputy Director of Finance & Performance	Information Governance and Data Protection Officer	09/10/2009
0.6	Alterations to Risk acceptance.	Comments from ICT & IG Programme Group	Information Governance and Data Protection Officer	14/12/2009
1.0	N/A	Ratified by CEO	Information Governance and Data Protection Officer	25/02/2010
1.1	"To Be Read With" section updated to refer to Information Governance Policy	Audit Recommendations	Information Governance and Data Protection Officer	12/10/2010

Table of Contents

1.	Introduction	4
2.	Scope.....	4
3.	Objectives	4
4.	Principles	5
5.	Responsibilities	7
5.1	Accountable Officer (Chief Executive)	7
5.2	Senior Information Risk Owners (Director of Finance and Performance, NHS Brent; Deputy Director of Finance and Performance Brent Community Services)	7
5.3	Brent Community Services (BCS)	7
5.4	Information Asset Owners/Administrators	7
5.5	All Staff	7
6.	SIRO Support Infrastructure.....	8
7.	Equality Impact Assessment	8
8.	Monitoring and Review.....	8
	Appendix 1 - Equality Impact Assessment Toolkit	9
	Appendix 2 - Audit Tool For The Information Risk Policy.....	11
	Appendix 3 - Assurance Form	12
	Appendix 4 - Policy Ratification and Publication	13

1. Introduction

- 1.1 This policy documentation sets out the PCT's Information Risk Policy.
- 1.2 This policy lays the framework for a formal information risk management programme in the PCT by explicitly establishing responsibility for information risk identification and analysis, planning for information risk mitigation, information risk management and its oversight.
- 1.3 It should be noted that this policy complements the PCT's Risk Management Strategy and Policy, and does not supersede this relevant documentation.
- 1.4 The responsibilities, definitions, processes and templates as contained in the PCT's overall Risk Management Strategy and Policy therefore also apply to the workings of this Information Risk Policy.

2. Scope

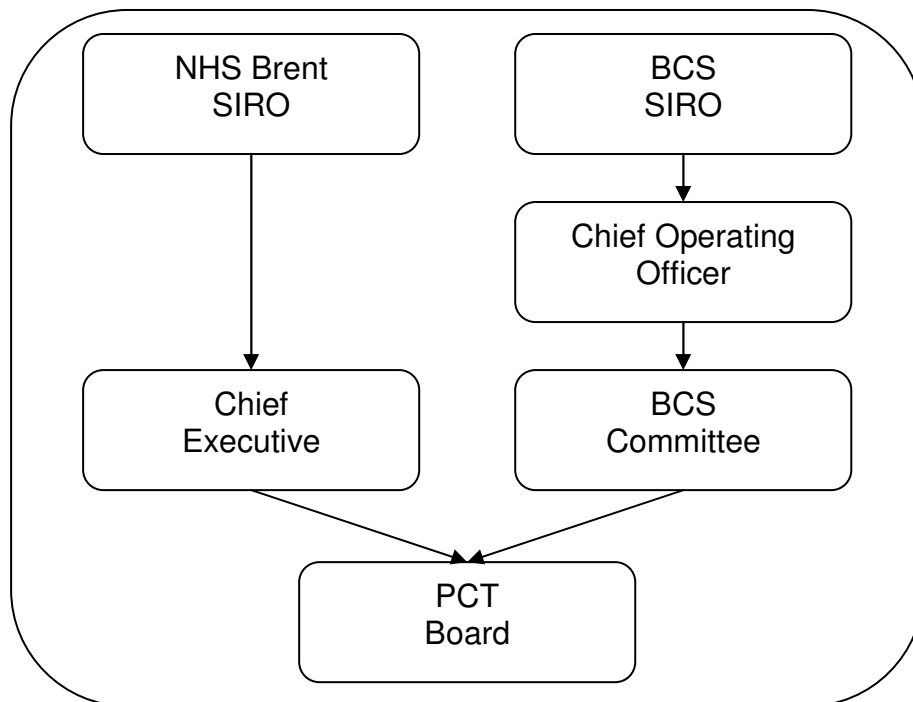
- 2.1 This policy applies to all departments and functions of the PCT and adherence should be observed by all staff, contractors and partner organisations working on behalf of the PCT. There are no exclusions.

3. Objectives

- 3.1 The Information Risk Policy has been created to:
 - Protect the PCT, its staff and its patients from information risks where the likelihood of occurrence and the consequences are significant;
 - Provide a consistent risk management framework in which information risks will be identified, considered and addressed in key approval, review and control processes;
 - Encourage pro-active rather than re-active risk management;
 - Provide assistance to and improve the quality of decision making throughout the PCT;
 - Meet legal or statutory requirements, and NHS Policy requirements;
 - Assist in safeguarding the PCT's information assets (Information, Software, Physical, Services, People, Others Less Tangible).
- 3.2 The purpose of this policy is to formally establish the PCT's position regarding its information risk management process. The intent is to embed information risk management in a very practical way into business processes and functions via key approval processes, review processes and controls, and not to impose information risk management as an extra requirement.

4. Principles

- 4.1 The PCT has two Senior Information Risk Owners (SIROs); one for NHS Brent operations, and one for Brent Community Services (BCS) operations. The SIROs are responsible for coordinating the development and maintenance of information risk management policies, procedures and standards for their respective operations of the PCT.
- 4.2 The SIROs shall advise the Chief Executive and the PCT Board on information risk management strategies and provide periodic reports and briefings on Program progress.



- 4.3 The SIROs are responsible for the ongoing development and day-to-day management of the PCT's Risk Management Programme for information privacy and security.
- 4.4 The PCT's Information Asset Owners (IAOs) and Information Asset Administrators (IAA) with delegated responsibility shall ensure that information risk assessments are performed at least annually on all information assets where they have been assigned 'ownership', following guidance from the SIROs on assessment method, format, content, and frequency. IAAs shall submit the risk assessment results and associated mitigation plans to their SIRO for review, along with details of any assumptions or external dependencies. Mitigation plans shall include specific actions with expected completion dates, as well as an account of residual risks.

- 4.5 The PCT will undertake an annual information flow mapping exercise and from this exercise determine the information risks regarding its data flows within the organisation and/or with its delivery partners.
- 4.6 The reporting of information (including Information Security) risks and incidents will be in line with the PCT's overall risk management and incident reporting processes.
- 4.7 The PCT is not willing to accept unmanaged or unnecessary information risks that may result in reputation damage, financial loss or exposure, major breakdown in information system or information integrity, significant incidents of regulatory non-compliance.
- 4.8 The PCT recognises that the outcome of information risk management approach may not eliminate information risk totally, but rather provide the organisation means to identify, prioritise and manage the risks and provide a balance between the cost of managing and treating risks, and the anticipated benefits that will be derived.

5. Responsibilities

5.1 Accountable Officer (Chief Executive)

The Chief Executive as Accountable Officer of the PCT has overall accountability and responsibility for Information Governance in the PCT and is required to provide assurance, through the Statement of Internal Control that all risks to the PCT, including those relating to information, are effectively managed and mitigated.

5.2 Senior Information Risk Owners (Director of Finance and Performance, NHS Brent; Deputy Director of Finance and Performance Brent Community Services)

- To delegate responsibilities to appropriate Information Asset Owners/Administrators within their organisational unit.
- To oversee the development of an Information Risk Policy, and a Strategy for implementing the policy within the existing Information Governance Framework.
- To take ownership of risk assessment process for information risk, including review of the annual information risk assessment to support and inform the Statement of Internal Control.
- To review and agree action in respect of identified information risks.
- To ensure that the PCT's approach to information risk is effective in terms of resource, commitment and execution and that this is communicated to all staff.
- To provide a focal point for the resolution and/or discussion of information risk issues within their organisational unit.

5.3 Brent Community Services (BCS)

The Brent Community Services SIRO will report information risk matters to the Chief Operating Officer and the BCS Committee. The BCS Committee will in turn report BCS information risks to the PCT Board.

5.4 Information Asset Owners/Administrators

Information Asset Owners (IAOs) are accountable to the SIRO and will provide assurance that information risk is being identified and managed effectively for those information assets that they have been assigned ownership. Information Asset Administrators (IAAs) will usually be staff who have day-to-day responsibility for management of information risks affecting one or more assets, and report these to the IAOs.

5.5 All Staff

All members of staff have a responsibility to ensure the effectiveness of risk management within the Trust. Please see the Risk Management Strategy and Policy for further details.

6. SIRO Support Infrastructure

- 6.1 The following roles will form the supporting infrastructure for the SIRO in matters of information risk across the PCT:
- Caldicott Guardian
 - Head of ICT
 - Business Systems Manager
 - Information Governance and Data Protection Officer
 - BCS Risk Manager
 - Head of Corporate Affairs (NHS Brent Only)
 - BCS Head of Governance (Brent Community Services Only)

7. Equality Impact Assessment

See Appendix 1.

8. Monitoring and Review

This policy will be reviewed once a year by the ICT & IG Programme Group. Auditing of this document should be done at least every two years based on monitoring the effectiveness of the policy in line with legislation and guidelines etc. An Audit Tool (Appendix 2) or Key Performance Indicator (KPI) will be used for monitoring purposes. The document Assurance Form (Appendix 3) will be used by Managers to document embedding of policies.

Appendix 1 - Equality Impact Assessment Toolkit

DOCUMENT AUTHOR	DIRECTORATE
NAME OF DOCUMENT/POLICY/STRATEGY/PROCEDURE	NEW EXISTING ASSOCIATED POLICIES, STRATEGIES OR PROCEDURES
DATE	

Aim/Status

[a] What is the aim/purpose of the policy/strategy/procedure?
[b] Who is intended to benefit from this policy/strategy/procedure and in what way?
[c] How have they been involved in the development of this policy/strategy/procedure?
[d] How does it fit into the broader corporate aims?
[e] What outcomes are intended from this policy/strategy/procedure?
[f] What resource implications are linked to this policy/strategy/procedure?

Impacts

[a] what is the likely impact [whether intended or unintended, positive or negative] of the initiative on individual users or on the public at large?		
[b] Is there likely to be differential impact on any group? If yes, please state if this impact may be adverse and give further details [e.g. which specific groups are affected, in what way, and why you believe this to be the case]		
[i] Grounds of race, ethnicity, colour, nationality or national origin	Please tick box yes <input type="checkbox"/> no <input type="checkbox"/>	Please tick box Adverse? <input type="checkbox"/> Please give further details
[ii] Grounds of sex or marital Status Women and Men	yes <input type="checkbox"/> no <input type="checkbox"/>	Adverse? <input type="checkbox"/> Please give further details

[iii] Grounds of gender: Transgender or Transsexual People	yes <input type="checkbox"/> no <input type="checkbox"/>	Adverse? <input type="checkbox"/> Please give further details
[iv] Grounds of religion or belief: Religious /faith or other Groups with a recognised belief system	yes <input type="checkbox"/> no <input type="checkbox"/>	Adverse? <input type="checkbox"/> Please give further details
[v] Grounds of disability	yes <input type="checkbox"/> no <input type="checkbox"/>	Adverse? <input type="checkbox"/> Please give further details
[vi] Grounds of age: Older people, children and Young people	yes <input type="checkbox"/> no <input type="checkbox"/>	Adverse? <input type="checkbox"/> Please give further details
[vii] Grounds of sexual orientation: Lesbian, gay, bisexual	Yes <input type="checkbox"/> no <input type="checkbox"/>	Adverse? <input type="checkbox"/> Please give further details
[viii] Grounds of carers: Older relatives, children	yes <input type="checkbox"/> no <input type="checkbox"/>	Adverse? <input type="checkbox"/> Please give further details
[ix] Grounds of human rights	yes <input type="checkbox"/> no <input type="checkbox"/>	Adverse? <input type="checkbox"/> Please give further details
Is the policy directly discriminatory? yes <input type="checkbox"/> no <input type="checkbox"/>	Is the policy indirectly discriminatory? yes <input type="checkbox"/> no <input type="checkbox"/> If you said yes, is this objectively justifiable or proportionate in meeting a legitimate aim yes <input type="checkbox"/> no <input type="checkbox"/>	Is the policy intended to increase equality of opportunity by permitting positive action or action to redress disadvantage yes <input type="checkbox"/> no <input type="checkbox"/> Please give details.
If the policy is unlawfully discriminatory it must go to a full impact assessment (please Contact the Equality, Diversity & Human Rights Advisor – Human Resources Directorate)		
Persons conducting EqIA		
Signed		Date

If you have identified a potential discriminatory impact of this procedural document, please refer it to the Equality & Diversity Manager together with any suggestions as to the action required to avoid/reduce this impact.

For advice in respect of answering the above questions, please contact the Equality & Diversity Manager.

Appendix 2 - Audit Tool For The Information Risk Policy

The following are five questions to assess your understanding and implementation of this policy

(Score yourself - Yes or No)

Do you understand the different definition of documents within the policy?	Yes / No
Do you understand the requirement for the main body of a document?	Yes / No
Do you understand the Ratification Process for documents?	Yes / No
Do you understand the Guidance on the Checklist required for writing documents?	Yes / No
Do you understand the process for reviewing / Archiving / consultation and version control?	Yes / No

If you score No for any of the questions, please re read the relevant section of the policy. If you are still unclear please contact the author / service for clarification

A copy of this **should** be kept in your personal file and may be used as part of a continuous profession development folder.

Signed..... **Role**.....

Date.....

Appendix 4 - Policy Ratification and Publication

Policy Title (including version)		Date
Information Risk Policy 1.1		12 October 2010
Reason for Submission (Please Tick)		
Scheduled Review	<input type="checkbox"/>	New Policy <input type="checkbox"/>
Urgent Amendments (Please specify)	<input checked="" type="checkbox"/>	Other <input type="checkbox"/>
<input type="text"/>		
Purpose of Policy		
This policy lays the framework for a formal information risk management programme in the PCT by explicitly establishing responsibility for information risk identification and analysis, planning for information risk mitigation, information risk management and its oversight.		
Supporting Evidence Please state list of reviewers/stakeholders and their job title (use a separate sheet if required) along with evidence of their participation in the review/creation of the policy.		
Previous Reviewers: Jonathan Wise, Director of Finance & Performance (NHS Brent's Senior Information Risk Owner) Henry Black, Deputy Director of Finance & Performance (Brent Community Services' Senior Information Risk Owner) Bridget Pratt, Head of Corporate Affairs Avtar Ubbi, Business Systems Manager		
New Policy: (Please reference sources of Best Practice used, and list applicable legislation)		
N/A		
Reviewed/Amended Policy: (Please provide full details of changes made, reference sources of Best Practice used, and list applicable legislation)		
"To Be Read With" section updated to refer to Information Governance Policy		
Policy Equality Impact assessed		
TBC		
Policy Approval		
Name:	Jonathan Wise, Acting Chair of ICT & IG Programme Group	
Signature:		
Date:	12 October 2010	
Policy Publication		
Date policy is uploaded on the intranet via the Communications Department		
TBC		
Policy to be emailed to Heads of Services to discuss at team meetings and staff forums (specify date)		
TBC		
Policy to be audited annually (Specify date of audit)		
TBC		