

Information Governance Policy

Version	2.0
Status	Ratified
Author/Lead	Information Governance & Data Protection Officer
Directorate	Finance and Performance
Ratified By	ICT & Information Governance Programme Group
Implementation Date	03 September 2010
Date of Last Review Date	08 July 2010
Date of Next Review	04 September 2011
Target Audience	All Staff

To be read with:

- Confidentiality and Data Protection Policy
- Acceptable Use of E-mail Policy
- Acceptable Use of The Internet Policy
- Acceptable Use of Information Systems Policy
- Information Security Policy
- Freedom of Information Policy
- Safe Haven Policy
- Bulk Transfer of (Electronic) Patient Records Policy
- Serious Untoward Incident Policy

“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
0.2	Initial Draft		Informatics Manager	29/09/2005
0.3		Incorporated the Informatics Programme Board's requested changes	Informatics Manager	29/09/2005
1.0	No Changes	Approved by Trust Board	Informatics Manager	17/11/2005
1.1	Policy Update	Annual Review	Business Systems Manager	07/02/2008
1.2	Minor update to reflect requirements of Policy Development Policy	Annual Review	Information Governance and Data Protection Officer	07/04/2009
1.3		Approved by ICT & IG Programme Group	Information Governance and Data Protection Officer	05/06/2009
1.4	Disciplinary Section Added.	Annual Review	Information Governance and Data Protection Officer	21/06/2010
2.0	Comments added from Reviewers	Annual Review and to take into account the Provider/ Commissioning split.	Information Governance & Data Protection Officer	08/07/2010

Table of Contents

1.	Introduction	4
2.	Purpose.....	4
3.	Scope.....	4
4.	Principles	5
4.1	Openness	5
4.2	Legal Compliance.....	6
4.3	Information Security.....	6
4.4	Information Quality Assurance.....	6
5.	Responsibilities	7
5.1	Board.....	7
5.2	ICT and Information Governance Programme Group.....	7
5.3	Managers	7
5.4	All Staff	7
6.	Disciplinary Procedures	7
7.	Monitoring and Review.....	7
	Appendix 1 - Equality Impact Assessment Tool.....	8
	Appendix 2 - Audit Tool For The Information Governance Policy	10
	Appendix 3 - Assurance Form	11
	Appendix 4 - Policy Ratification and Publication	12

1. Introduction

- 1.1 Information is a vital asset, both in terms of the clinical management of individual patients and the efficient management of services and resources. It plays a key part in clinical governance, service planning and performance management.
- 1.2 It is therefore of paramount importance to ensure that information is efficiently managed, and that appropriate policies, procedures and management accountability and structures provide a robust governance framework for information management.

2. Purpose

- 2.1 NHS Brent acknowledges that information is a valuable asset, therefore it is wholly in its interest to ensure that the information it holds, in whatever form, is appropriately governed, protecting the interests of all of its stakeholders.
- 2.2 This policy, and its supporting standards and work instruction, are fully endorsed by the Board through the production of these documents and their minuted approval.

3. Scope

- 3.1 This policy applies to all employees of NHS Brent and Brent Community Services (BCS), including contracted and temporary staff.
- 3.2 All staff, contractors, and other relevant parties will ensure that these are observed in order that we may contribute to the achievement of the PCT's objectives and the delivery of effective healthcare to the local population.

4. Principles

The Trust recognises the need for an appropriate balance between openness and confidentiality in the management and use of information. The Trust fully supports the principles of corporate governance and recognises its public accountability, but equally places importance on the confidentiality of, and the security arrangements to safeguard, both personal information about patients and staff and commercially sensitive information. The Trust also recognises the need to share patient information with other health organisations and other agencies in a controlled manner consistent with the interests of the patient and, in some circumstances, the public interest.

The Trust believes that accurate, timely, and relevant information is essential to deliver the highest quality health care. As such it is the responsibility of all clinicians and managers to ensure and promote the quality of information and to actively use information in decision making processes.

There are 4 key interlinked strands to the information governance policy:

- Openness
- Legal compliance
- Information security
- Quality assurance

4.1 Openness

- Non-confidential information on the Trust and its services should be available to the public through a variety of media, in line with the Trust's code of openness.
- The Trust will establish and maintain policies to ensure compliance with the Freedom of Information Act.
- The Trust will undertake or commission annual assessments and audits of its policies and arrangements for openness.
- Patients should have ready access to information relating to their own health care, their options for treatment and their rights as patients.
- The Trust will have clear procedures and arrangements for liaison with the press and broadcasting media.
- The Trust will have clear procedures and arrangements for handling queries from patients and the public.

4.2 Legal Compliance

- The Trust regards all identifiable personal information relating to patients as confidential.
- The Trust will undertake or commission annual assessments and audits of its compliance with legal requirements.
- The Trust regards all identifiable personal information relating to staff as confidential except where national policy on accountability and openness requires otherwise.
- The Trust will establish and maintain policies to ensure compliance with the Data Protection Act, Human Rights Act and common law confidentiality.
- The Trust will establish and maintain policies for the controlled and appropriate sharing of patient information with other agencies, taking account of relevant legislation (e.g. Health and Social Care Act, Crime and Disorder Act, Protection of Children Act).

4.3 Information Security

- The Trust will establish and maintain policies for the effective and secure management of its information assets and resources.
- The Trust will undertake or commission annual assessments and audits of its information and IT security arrangements.
- The Trust will promote effective confidentiality and security practice to its staff through policies, procedures and training.
- The Trust will establish and maintain incident reporting procedures and will monitor and investigate all reported instances of actual or potential breaches of confidentiality and security.

4.4 Information Quality Assurance

- The Trust will establish and maintain policies and procedures for information quality assurance and the effective management of records.
- The Trust will undertake or commission annual assessments and audits of its information quality and records management arrangements.
- Managers are expected to take ownership of, and seek to improve, the quality of information within their services.
- Wherever possible, information quality should be assured at the point of collection.
- Data standards will be set through clear and consistent definition of data items, in accordance with national standards.
- The Trust will promote information quality and effective records management through policies, procedures/user manuals and training.

5. Responsibilities

5.1 Board

It is the role of the Trust Board to define the Trust's policy in respect of Information Governance, taking into account legal and NHS requirements. The Board is also responsible for ensuring that sufficient resources are provided to support the requirements of the policy.

5.2 ICT and Information Governance Programme Group

The ICT and Information Governance Programme Group is responsible for overseeing day to day Information Governance issues; developing and maintaining policies, standards, procedures, and guidance, coordinating Information Governance in the Trust and raising awareness of Information Governance.

5.3 Managers

Managers within the Trust are responsible for ensuring that the policy and its supporting standards and guidelines are built into local processes and that there is on-going compliance.

5.4 All Staff

All staff, whether permanent, temporary or contracted, and contractors are responsible for ensuring that they are aware of the requirements incumbent upon them and for ensuring that they comply with these on a day to day basis.

To monitor staff awareness, and in line with the NHS Operating Framework – 'Informatics Planning 2010/11', the PCT will provide annual IG Training through the use of the NHS IG Training Tool.

6. Disciplinary Procedures

- 6.1 All suspected breaches of this policy will be investigated and may be subject to the Trust's formal disciplinary procedures. Serious breaches may result in immediate suspension and/or termination of contract, under the PCT Performance and Conduct Policy and the Serious Untoward Incident Policy.

7. Monitoring and Review

- 7.1 This policy will be reviewed once a year by ICT. 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) 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 Tool

To be completed and attached to any procedural document when submitted to the appropriate committee for consideration and approval.

Summary

Document Author	Information Governance & Data Protection Officer
Directorate	Finance and Performance
Name of Document / Policy / Strategy / Procedure	Information Governance Policy
Document Status	New Document <input type="checkbox"/> Existing Document <input checked="" type="checkbox"/>
Associated Policies, Strategies or Procedures	<ul style="list-style-type: none"> • Confidentiality and Data Protection Policy • Acceptable Use of E-mail Policy • Acceptable Use of The Internet Policy • Acceptable Use of Information Systems Policy • Information Security Policy • Freedom of Information Policy • Safe Haven Policy • Bulk Transfer of (Electronic) Patient Records Policy
Date	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 checked="" 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 checked="" type="checkbox"/>	Adverse? <input type="checkbox"/> Please give further details
[iii] Grounds of gender: Transgender or Transsexual People	Yes <input type="checkbox"/> No <input checked="" 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 checked="" type="checkbox"/>	Adverse? <input type="checkbox"/> Please give further details
[v] Grounds of disability	Yes <input type="checkbox"/> No <input checked="" 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 checked="" type="checkbox"/>	Adverse? <input type="checkbox"/> Please give further details
[vii] Grounds of sexual orientation: Lesbian, gay, bisexual	Yes <input type="checkbox"/> No <input checked="" type="checkbox"/>	Adverse? <input type="checkbox"/> Please give further details
[viii] Grounds of carers: Older relatives, children	Yes <input type="checkbox"/> No <input checked="" type="checkbox"/>	Adverse? <input type="checkbox"/> Please give further details
[ix] Grounds of human rights	Yes <input type="checkbox"/> No <input checked="" type="checkbox"/>	Adverse? <input type="checkbox"/> Please give further details
Is the policy directly discriminatory? Yes <input type="checkbox"/> No <input checked="" type="checkbox"/>	Is the policy indirectly discriminatory? Yes <input type="checkbox"/> No <input checked="" 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 Governance 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 Governance Policy 2.0		08/07/2010
Reason for Submission (Please Tick)		
Scheduled Review	<input checked="" type="checkbox"/>	New Policy <input type="checkbox"/>
Urgent Amendments (Please specify)	<input type="checkbox"/>	Other <input type="checkbox"/>
<input type="text"/>		
Purpose of Policy		
This policy outlines the PCT's commitment to the information governance framework.		
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.		
Reviewers: <ul style="list-style-type: none"> • Head of ICT • Business Systems Manager • Information Governance & Data Protection Officer • Head of Information (NHS Brent) • Head of Governance (BCS) 		
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)		
Sources of Best Practice Used: <ul style="list-style-type: none"> • NHS CFH Exemplar Trust IG Policy available on CfH IG Toolkit KnowledgeBase • Policy Development Policy 		
Amendments: <ul style="list-style-type: none"> • Policy Development Policy format. • Disciplinary section added. 		
Policy Equality Impact assessed		
TBC		
Policy Approval		
Name:	Chair of ICT & IG Programme Group	
Signature:		
Date:		
Policy Publication		
Date policy is uploaded on the intranet via the Communications Department		
TBC		
Policy to be e-mailed to Heads of Services to discuss at team meetings and staff		
TBC		
Policy to be audited annually		
TBC - Results to be fed back to ICT & IG Programme Group		