

Confidentiality and Data Protection 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:

- Safe Haven Policy
- Procedure on the decommissioning and disposal of computer equipment
- Bulk Transfer of (Electronic) Patient Records Policy
- Privacy Impact Assessment Policy
- Access to Health 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
1.0	Confidentiality Policy integrated in this document		Remi Ogbe	13/01/2006
1.0	Suggestions from ICT Dept. inserted in document – Approved by IMT ICT Dept.		Remi Ogbe	02/02/2006
1.0	Comments from Patricia A incorporated – Approved by IMT ICT Dept.		Remi Ogbe	24/02/2006
1.0	Comments from IG Steering Group incorporated – Approved by IG Steering Group		Remi Ogbe	05/04/2006
1.1	Minor amendments made to sharepoint links – Approved by Caldicott Guardian & IG SG	Annual Review	Business Systems Manager	21/01/2008
1.2	Minor Changes and update to Information For Patients, Carers, Service Users And Staff	Annual Review and Standards for Better Health compliance. To bring policy in line with Policy Development Policy.	Information Governance and Data Protection Officer	27/02/2009
1.3	Hyperlink updates. Update for Policy Development Policy requirements. Updated scope. Reference made to Privacy Impact Assessment Policy	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.	General Principles	5
5.	Type of Information Held By The Trust.....	5
6.	Information For Patients, Carers, Service Users And Staff	6
7.	Disclosure Of Information	7
8.	Security Measures And Access Controls	9
9.	Training and Development	10
10.	Using Information In The Prevention, Detection And Prosecution Of Serious Crime.....	10
11.	Media	11
12.	Audit.....	11
13.	Record Logs.....	11
14.	Procurement And Implementation Of New Information Systems	12
15.	Disciplinary Procedures.....	12
16.	Monitoring and Review	12
	Appendix 1 - Equality Impact Assessment Tool	13
	Appendix 2 - Audit Tool For The Confidentiality and Data Protection Policy.....	15
	Appendix 3 - Assurance Form.....	16
	Appendix 4 - Policy Ratification and Publication.....	17

1. Introduction

- 1.1 On the 1st March 2000 the 1998 Data Protection Act (the Act) became law. The Act replaced the 1984 Act and the Access to Health Records Act 1990 in respect of living persons and provides the legal framework to deliver the requirements of the recommendations of the Information Governance Toolkit.
- 1.2 The 1998 Data Protection Act includes manual data if the data forms part of a paper based personal data filing system structured to specific criteria relating to individuals, allowing easy access to personal data. Sound and image data are included as is the collection, retrieval, destruction and use of such data, whether done manually or electronically. The Freedom of Information Act 2000 has made a number of amendments to the Data Protection Act 1998. One of the most significant is that the definition of 'data' is extended, as far as public authorities are concerned, to cover all personal information held. This will include 'structured' and 'unstructured' manual records.
- 1.3 The principle aim of the 1998 Data Protection Act is to enhance the individual's right to privacy with respect to the processing of personal data and ensure that processing is done in accordance with the rights of the individual.

2. Purpose

- 2.1 This policy provides the framework for how the organisation will use information systems (both computerised and paper-based) in the most secure, appropriate and responsible way.
- 2.2 For further guidelines see: <http://www.informationcommissioner.gov.uk/>

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 The scope of this policy is to cover Data Protection Act requirements and also the application of the Confidentiality Code of Practice in NHS Brent. Please note that this Policy refers to the Trust's DPA registration and not to individual GP Practices. They have their own DPA Registration and policies.
- 3.3 The principle aim of the Act is to strengthen the individual's right to privacy with respect to the processing of personal data and ensure that processing is done in accordance with the rights of the individual.

4. General Principles

- 4.1 The NHS Brent (*the Trust*) will take all reasonable action necessary to maintain the **confidentiality, integrity and availability** of its information processing.
- 4.2 The Trust's information processing is bound by the six **Caldicott principles** which govern the use of patient-identifiable information in the NHS:
- i. Justify the purpose.
 - ii. Don't use patient identifiable information unless it is absolutely necessary.
 - iii. Use the minimum necessary patient identifiable information.
 - iv. Access to patient identifiable information should be on a strict need to know basis.
 - v. Everyone should be aware of their responsibilities.
 - vi. Understand and comply with the law.
- 4.3 Patient identifiable information must not be disclosed either verbally or in writing to unauthorised persons. It is particularly important that staff should ensure the authenticity of telephone enquiries.
- 4.4 All information held by the Trust will be obtained and processed fairly and in accordance with health service guidance and government legislation.
- 4.5 The information collected and held by the Trust will be used only for those purposes specified in the Trust's formal registration under the Data Protection Act. (<http://www.ico.gov.uk/ESDWebPages/search.asp>)
- 4.6 All of the Trust's employees have an individual responsibility for keeping up-to-date on issues of security, data protection and confidentiality and are required to undertake awareness training appropriate to the responsibilities of their post.

5. Type of Information Held By The Trust

- 5.1 The information held by the Trust will be adequate, relevant to its stated needs and purposes, and not excessive. It will not be held any longer than is necessary or required by law.
- 5.2 The Trust will make every reasonable effort to ensure that the information it holds is accurate and up-to-date, as appropriate. It will amend any errors in the information it holds.
- 5.3 The Information Commissioner's Office (ICO) is the regulatory body that monitors compliance with the Data Protection Act. The PCT has a duty to inform the ICO how it processes personal data.

6. Information For Patients, Carers, Service Users And Staff

- 6.1 The Data Protection Principles sets out the obligation on Data Controllers (Trust staff who have the data) to provide certain information to Data Subjects (patients, service users, staff) when collecting their personal data:
- **The identity of the Data Controller(s);**
Information as to the identity of the Data Controller should be reasonably specific (e.g. the GPs practice, the Trust etc). “The NHS” or “The Health Service” are not legal entities and therefore cannot be Data Controllers.
 - **The identity of any representative nominated by the Data Controller for the purposes of the Act;**
Data Controllers must also be aware that with increased multi-agency working and initiatives (e.g. between the Trust and a social services department), it may not be immediately clear to Data Subjects as to who the Data Controller actually is. Indeed, there may be more than one Data Controller, in which case the identity of all Data Controllers should be communicated to Data Subjects.
 - **The purpose(s) for which the data are to be processed;**
When explaining the purpose(s) for which information is to be processed, Data Controllers must strike a balance between providing an unnecessary amount of detail and providing information in too general terms. An explanation to the effect that personal data are to be processed for ‘health care purposes’ would be too general: on the other hand, an explanation that explained all the administrative systems in which patient data might be recorded, the use of data for diagnosis, for treatment etc would be excessive. (An explanation which is not sufficiently detailed is unlikely; in any event, to be sufficient to obtain the consent of the Data Subject to the processing of data should this be required.
 - **Any further information which is necessary, having regard to the specific circumstances in which the data are or are to be processed, to enable the processing in respect of the Data Subject to be fair.**
- 6.2 Healthcare professionals of the Trust providing patient care are responsible for informing the patient of how their personal information will be recorded and for what purpose. They should also explain to patients / carers of the importance for providing accurate information and ensuring all changes to the information in the future is provided.

- 6.3 Most uses or disclosures of medical data will be justified by having obtained the consent from the patients:
- **Firstly, consent must be informed.**
The Data Subject must know what are the proposed uses or disclosures of personal data.
 - **Secondly, the person giving consent must have some degree of choice.**
“Consent” given under duress or coercion is not consent at all.
 - **Thirdly, there must be some indication that the Data Subject has given his or her consent.**
Healthcare professionals of the Trust providing patient care are therefore instructed to discuss with patients / carers, dependent on the ability of the patient to consent, the personal information they collect and how that information will be used. Healthcare professionals must then record the conversation and whatever consent they obtain, in the patients medical record.

7. Disclosure Of Information

- 7.1 The information held by the Trust will not be shared with any other parties except in accordance with the disclosure clauses set out in its formal **Data Protection Registration** <http://www.ico.gov.uk/ESDWebPages/search.asp>
- 7.2 The information held by the Trust will not be shared with any other parties except in accordance with the disclosure clauses set out in the London Borough of Brent Overarching inter-agency **Information Sharing Protocol**. Where Trust Services need to share information to other than Brent agencies an appropriate Info Sharing protocol needs to be drawn up. The ICT Department is prepared to assist in this matter.
- 7.3 The number and type of data items which could allow identification on an individual will be reduced to the minimum essential for the purpose. Data, wherever practical, will be anonymised.
- 7.4 All data flows, existing or planned, will be tested against the basic principles of good practice. Existing data flows will be reviewed regularly to ensure that they remain compatible with these principles.
- 7.5 In case information needs to be shared with other health or social work practitioners all reasonable action will be undertaken to make sure that the information will be kept in strict professional confidence and be used only for the purpose for which the information was given and collected.
- 7.6 The Trust will ensure that they share information in accordance with their statutory duties including the requirements of the Data Protection Act 1998 and the Human Rights Act 1998. Wherever possible and appropriate, the Trust will seek consent from the service user to share personal information. The service user or Data Subject will be made fully aware of the information it is proposed to share and the purposes for which it will be used.

- 7.7 Patients will generally be asked for consent before their personal information is used in ways that not directly contribute to, or support the delivery of their care.
- 7.8 The Trust will put procedures in place to ensure that decisions to share personal information without consent have been fully considered and comply with the requirements of the relevant legislation. Such decisions will be appropriately recorded for audit purposes. All staff will be made aware of the roles and responsibilities of the Data Protection Officer and/or the Caldicott Guardian should they need advice regarding sharing without consent.
- 7.9 Judgements regarding disclosure and information sharing will be based on a '*minimum need-to-know*' principle; the final decision will rest with the [Caldicott Guardian](#). Caldicott Guardians are senior staff in the NHS and social services appointed to protect patient information. The PCT's Caldicott Guardian is the PCT's Medical Director. The Caldicott Guardian will be assisted by the ICT Department in addressing confidentiality issues related to information systems.
- 7.10 Under the Data Protection Act patients and staff have the right to receive copies of any information held electronically and any manual record made about them: they also have the right to view such records. There are exclusions to this general right. Requests to access these records are to be made to the PCT's Corporate Affairs department (for patient records) and Human Resources Manager (for staff records).
- 7.11 Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of Data Subjects in relation to the processing of personal data the DPA does not impose any restrictions on the transfer of personal data to EEA countries. It should be remembered that the Channel Islands and the Isle of Man are not part of the EEA.
- 7.12 Transfers to countries outside the EEA can be made with the consent of the Data Subject. Consent must be freely given.
- 7.13 Transfers can be made where they are necessary in order to protect the vital interests of the Data Subject. This relates to matters of "life and death". For example, it would cover the transfer of relevant medical records from the UK to another country where an individual had been taken seriously ill or involved in a serious accident.
- 7.14 Judgements regarding disclosure and information sharing will be based on a '*minimum need-to-know*' principle; the final decision will rest with the Caldicott Guardian.

8. Security Measures And Access Controls

- 8.1 The Trust will have appropriate security measures in place to guard data against:
- *unauthorised access to, alteration, disclosure, and destruction.*
 - *accidental loss or destruction.*
- 8.2 The Trust will ensure, through its documented procedures that only authorised individuals can gain access to its systems and records (role based access).
- 8.3 Conversations and/or screens relating to confidential matters affecting patients should not take place in situations where they may be overheard or viewed by passers-by, e.g. in corridors, reception areas, lifts etc. The same confidentiality must also be preserved in dealing with work related matters appertaining to work colleagues.
- 8.4 The Trust will ensure, wherever possible, that the NHS Number is used in place of other personal identifiers, as a means of:
- *preserving a higher level of confidentiality for its patients and service users.*
 - *reducing the risk of revealing personal data through casual prying.*
- 8.5 All equipment, records and storage media will be protected from intruders by appropriate physical and electronic security measures.
- 8.6 All fax machines used for the sending or receipt of personal/confidential data will be placed in a secure location, a 'Safe Haven', to prevent casual browsing by unauthorised personnel.
- 8.7 The copying, archiving or transferring of any data, electronic or paper or other media, will be treated with the same level of security and access restrictions as applied to *live* data.
- 8.8 All paper-based records containing personal data will be shredded after use, or disposed of using the Trust's approved channels for the disposal of confidential/sensitive data within the guidelines / regulations on retention that apply to certain records.
- 8.9 Information held on electronic media will be permanently erased before the media is disposed of (*please see the procedure on the decommissioning and disposal of computer equipment*).
- 8.10 Back-ups of systems and data will be taken at regular, pre-determined intervals in accordance with the written procedures for each system.
- 8.11 The Trust will ensure that appropriate contingency plans are in place, tested and reviewed regularly, to enable information and systems to be restored as quickly as possible, following a system failure or theft.

9. Training and Development

- 9.1 All employees of the Trust will be made aware of their personal responsibility to keep up-to-date on issues of security, data protection and confidentiality.
- 9.2 The Trust will provide regular, on-going training for new and existing staff on security, data protection, Caldicott and records management.
- 9.3 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.
- 9.4 *Live* data will not be used for testing, training or demonstration purposes unless it has been transformed or anonymised to prevent identification of the individual and the contents of his/her record.

10. Using Information In The Prevention, Detection And Prosecution Of Serious Crime

- 10.1 The Trust will, under special circumstances, pass on patient identifiable information to help tackle serious crime. This will be justified if the following conditions are satisfied:
- Without the Trust's disclosure the task of preventing, detecting or prosecuting the crime could be seriously prejudiced or delayed.
 - The disclosure of information by the Trust will assist local partnerships to implement the provisions of the ***Crime and Disorder Act 1998***¹
 - The information released by the Trust is limited to what is strictly relevant to a specific investigation.
 - Decisions on disclosure are based on fact, and not rumour or supposition.
 - Decisions on disclosure are fully documented and justifiable in the event of legal challenge.
 - The Trust is satisfied that the information will be treated confidentially by the third party and will not be passed on or used for any purpose other than the investigation for which it was released.
- 10.2 The Trust will not generally consider requests for information relating to a number of patients in order to identify one or more specifically, unless there is a strong public interest to make it justifiable.
- 10.3 For its definition of *serious crime*, the Trust will work to the list of serious arrestable offences, specified in Section 116 of the Police and Criminal Evidence Act 1984.

¹ Note : Section 115 of the Crime and Disorder Act 1998 provides a statutory authority which enables the disclosure of personal information to be considered whenever it is necessary or expedient to the successful implementation of the Act

11. Media

- 11.1 Maintaining good relations with the media is important and all enquiries from the media to the Trust must be handled by the Head of Communications.
- 11.2 If a request for information concerns a particular patient, then the patient's consent must be obtained if he or she is capable of taking a decision.
- 11.3 Where the patient is unable to take a decision, providing basic information may sometimes be judged to be in his or her best interest (for example by correcting misleading information or damaging speculation) and the public interest. Wherever possible, relatives should be consulted. In all such circumstances, the Trust must be prepared and able to justify a decision to release information.
- 11.4 If a patient or former patient has invited the media to report his or her treatment, the Trust may comment in public, but should confine itself to factual information or correcting any misleading assertions or comments. The duty of confidence still applies.

12. Audit

- 12.1 The ICT Department, acting on behalf of the Trust and under guidance from the services, will undertake routine and special audits of quality, completeness of data held on computerised systems to ensure compatibility with the Data Protection Principles.
- 12.2 Any concerns regarding the integrity of data will be referred to service managers for action.

13. Record Logs

- 13.1 Managers and service heads will ensure that all changes to patient identifiable information (amendments, additions and deletions) are recorded and logged, on both computerised and paper-based systems, as a means of providing a reliable audit trail.
- 13.2 All persistent errors in the recording of information will be reported to the Service Manager, who will be responsible for determining the source of the problem and implementing the necessary corrective action.

14. Procurement And Implementation Of New Information Systems

- 14.1 When procuring new information systems and implementing new procedures, the Trust will actively consider the security implications and ensure that all necessary steps are taken to comply with the requirements set out in this policy.
- 14.2 The Trust will also consider service user privacy implications when introducing new information systems, and ensure that where appropriate a Privacy Impact Assessment will be undertaken in line with the Trust's Privacy Impact Assessment Policy.

15. Disciplinary Procedures

- 15.1 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.

16. Monitoring and Review

- 16 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) 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	Acceptable Use of Information Systems 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"> • Safe Haven Policy • Procedure on the decommissioning and disposal of computer equipment • Bulk Transfer of (Electronic) Patient Records Policy • Privacy Impact Assessment Policy • Access to Health Records Policy
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	<p style="text-align: center;">Please tick box</p> Yes <input type="checkbox"/> No <input checked="" type="checkbox"/>	<p style="text-align: center;">Please tick box</p> 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 Confidentiality and Data Protection 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
Confidentiality and Data Protection Policy 2.0	07/08/2010
Reason for Submission (Please Tick)	
Scheduled Review <input checked="" type="checkbox"/>	New Policy <input type="checkbox"/>
Urgent Amendments <input type="checkbox"/> (Please specify)	Other <input type="checkbox"/>
<input type="text"/>	
Purpose of Policy	
This policy outlines the Data Protection Act requirements and also the application of the Confidentiality Code of Practice at the PCT and how the organisation will use information systems (both computerised and paper-based) in the most secure, appropriate and responsible way.	
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"> • Policy Development Policy Amendments: <ul style="list-style-type: none"> • Policy Development Policy format. • Reference to Privacy Impact Assessment added. • 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	