

Pseudonymisation (De-identification) Policy

Version	1.0
Status	Ratified
Author/Lead	Information Governance & Data Protection Officer / Head of Information
Directorate	Finance and Performance
Ratified By	ICT & Information Governance Programme Group
Implementation Date	TBC
Date of Last Review Date	March 2011
Date of Next Review	February 2012
Target Audience	All Staff

To be read with:

- Acceptable Use of E-mail Policy
- Information Governance Policy
- Safe Haven Policy
- Bulk Transfer of (Electronic) Patient Records Policy
- Confidentiality and Data Protection Policy
- NHS Confidentiality Code of Practice
- Performance and Conduct Policy
- Serious 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
0.1	New Policy		ICT & Information Governance Programme Group	11/01/2011
0.2	Pseudonymisation Controls expanded	Input from Head of Information	ICT & Information Governance Programme Group	19/01/2011
1.0	Ratified	Ratification	ICT & Information Governance Programme Group	23/03/2011

Table of Contents

1.	Introduction	4
2.	Purpose.....	4
3.	Scope.....	4
4.	Definitions	5
5.	General Principles.....	6
6.	Responsibilities	7
7.	Training	8
8.	Pseudonymisation Controls	8
9.	Disciplinary Procedures	8
10.	Monitoring and Review.....	8
	Appendix 1 – Caldicott Authorisation to Access PID for Secondary Uses Form.....	9
	Appendix 2 - Caldicott Principles	11
	Appendix 3 - Equality Impact Assessment Tool.....	12
	Appendix 4 - Audit Tool For The Pseudonymisation (De-identification) Policy	14
	Appendix 5 - Assurance Form	15
	Appendix 6 - Policy Ratification and Publication.....	16

1. Introduction

- 1.1 It is NHS Policy and a legal requirement that, when patient data is used for purposes not involving the direct care of the patient, the patient should not be identified unless other legal means hold, such as the patient consent.
- 1.2 The NHS Confidentiality Code of Practice states the need to 'effectively anonymise' patient data prior to the non-direct care usage being made of the data.
- 1.3 Data itself cannot be labelled as primary or secondary use data, it is the purpose of the disclosure and the usage of the data that is either primary or secondary. This means that it is legitimate to hold data in identifiable form, but it becomes essential to ensure that only authorised users are able to have identifiable data disclosed to them.

2. Purpose

- 2.1 This policy provides the framework for how the organisation will use patient identifiable data for purposes other than the direct care of patients.

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.

4. Definitions

Term	Definition
Pseudonymisation / Pseudonymised Data	<p>Also known as de-identification, is the process involved to enable the NHS organisations to undertake secondary use of patient data in a legal, safe and secure manner.</p> <p>Pseudonymisation involves the removing of identifiers from patient data so that a patient/service user may not be identified.</p> <p>However where multiple sets of data are used, links should be enabled so that it is possible to analyse data sets and trends over time. Individual Service User activity should be able to be identified, but not the Service User themselves.</p>
Anonymised Data	<p>This is information which does not identify an individual directly, and which cannot reasonably be used to determine identity.</p> <p>Anonymisation does not allow information about the same individual to be linked in the same way that Pseudonymisation does.</p> <p>Anonymisation is more likely to be used for 'one-off' queries of data.</p>
Primary Use / Healthcare Purposes	<p>Primary use of patient data covers two types, those that directly contribute to the diagnosis, care and treatment of an individual and those used in the audit/assurance of the quality of healthcare provider.</p>
Secondary Use Purposes	<p>Where Patient Identifiable Data is used for work not directly related to the care of the patient/service user.</p> <p>Examples of secondary uses are commissioning, payment by results (PbR), performance management, capacity planning, service redesign and benchmarking.</p>
PID	<p>Person/Patient Identifiable Data (PID), also known as 'Identifiers'.</p> <p>PID essentially refers to any data, or combination of data, that can be used to identify an individual.</p> <p>These include, but are not limited to the following:</p> <p>Name - including last name and any forename or aliases</p> <ul style="list-style-type: none"> • Address – including any current or past address of residence • Date of birth • Postcode - including any current or past postcode of residence • NHS number • Ethnic category • Local Patient identifier • Patient pathway identifier • SUS spell ID • Unique booking reference number • Social Service Client number • Date of death

5. General Principles

- 5.1 Patient identifiable Data (PID) should generally only be used where:
 - There is a direct care-related need to use such data. Patient level data should not contain identifiers when they are used for purposes other than the direct care of patients.
 - Patient consent has been received.
 - Section 60/251 regulations apply for Public Health data.
- 5.2 When using PID for Secondary Use purposes, data must be anonymised / de-identified as much is practically possible.
- 5.3 Data itself cannot be labelled as primary or secondary use data, it is the purpose of the disclosure and the usage of the data that is either primary or secondary. This means that it is legitimate to hold data in identifiable form, but it becomes essential to ensure that only authorised users are able to have identifiable data disclosed to them.
- 5.4 Safe Haven procedures must be used at *all* times when handling and sharing PID, regardless of whether the data is being used for healthcare purposes or secondary use purposes.
- 5.5 Staff who have access to PID for Secondary Use purposes should be identified.
- 5.6 Access to PID for Secondary Use purposes should be appropriately authorised by the PCT's Caldicott Guardian.
- 5.7 Access to PID should be restricted to authorised users only.
- 5.8 A register of staff with access to PID for Secondary Use purposes should be created and maintained.
- 5.9 Staff access to PID for Secondary Use purposes should be periodically reviewed, to ensure that the level of access to PID is still relevant and appropriate.

6. Responsibilities

6.1 Managers

Managers must:

- Identify staff that have a justified purpose to access PID for Secondary Use purposes.
- Ensure that their staff are appropriately trained, utilising the Information Governance Training Tool.
- Regularly review the appropriateness of staff access to PID
- Organise the removal of staff access rights to PID, where there is no longer a need for staff to access PID for Secondary Use purposes.
- Inform the Information Governance & Data Protection Officer of staff that no longer require access to PID.
- Inform the Caldicott Guardian of new staff that require access to PID for Secondary Use purposes. The '*Caldicott Authorisation to Access PID for Secondary Uses Form*' in Appendix 1 should be completed and sent to the Caldicott Guardian for approval.

6.2 Staff

Staff with access to PID for Secondary Use purposes must:

- Keep PID confidential.
- Only use/transfer PID when authorised to do so.
- Transfer PID in a secure manner as per agreed Safe Haven procedures.
- When transferring PID via e-mail to another NHS organisation, NHSmail should be used by both sender and recipients. See the Acceptable Use of E-mail Policy for further details.
- All other transfers of PID should be via approved secure methods and/or secure networks.
- Anonymise PID where possible. In any case, the minimum amount of PID necessary should be used. See the Caldicott Principles in Appendix 2 for further details.

6.3 Caldicott Guardian

The Caldicott Guardian must:

- Review and authorise staff access to PID for Secondary Use Purposes.
- Inform the Information Governance & Data Protection Officer of staff approvals of access to PID for Secondary Use purposes. Completed '*Caldicott Authorisation to Access PID for Secondary Uses Form*' (Appendix 1) should be forwarded and filed by the Information Governance & Data Protection Officer.

6.4 Information Governance & Data Protection Officer

The Information Governance & Data Protection Officer must:

- Monitor Information Governance Training Tool records to ensure that staff with access to PID for Secondary Use purposes have completed the necessary training required.
- Maintain a register of staff who have access to PID for Secondary Use purposes.

7. Training

- 7.1 All staff that have access to Patient identifiable Data are required to complete the Introduction to Information Governance module on the online Information Governance Training Tool
- 7.2 The Information Governance Training Tool can be accessed here:
<http://www.igte-learning.connectingforhealth.nhs.uk/igte/index.cfm>

8. Pseudonymisation Controls

In addition to the PCT's Safe Haven and procedures and staff training through the IG Training Tool, the PCT currently employs the following Pseudonymisation Controls:

- 8.1 When data warehouse suppliers and systems are refreshed, Pseudonymisation controls and technology should be implemented where possible, including relevant logging and auditing facilities.
- 8.2 When releasing patient level data to other staff or third parties (for example consultancies employed by the PCT) where no data sharing arrangement is in place, information staff will deploy a Pseudonymisation algorithm to all patient identifiable data items. This will ensure there is linkage between records without compromising patient confidentiality. Pseudonymisation keys will not be released to staff outside of the Information Team and will be changed on a regular basis.

9. Disciplinary Procedures

- 9.1 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 Incident Policy.

10. Monitoring and Review

- 10.1 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 4) will be used for monitoring purposes. The document Assurance Form (Appendix 5) will be used by Managers to document embedding of policies.

Appendix 1 – Caldicott Authorisation to Access PID for Secondary Uses Form

This Form is to be completed by the relevant Service Manager when it is necessary for a member of staff to access Patient Identifiable Data (PID) for Secondary Use Purposes. This form should be sent to the Caldicott Guardian for authorisation and risk assessment.

Details of User Requesting Access to PID for Secondary Use Purposes

Name:.....

Email Address:..... Contact Number:.....

Department:..... Directorate:.....

Details of Data to be Accessed for Secondary Use Purposes

Data Description:

.....

.....

Types of Data User will be accessing:

Name D.o.B Gender

Ethnicity Medical Details Address

Other (please specify)

.....

.....

.....

Reason of Accessing PID

.....

.....

.....

Format of Data Transfer (i.e. electronic/paper based):

.....

Frequency of Data Access (i.e. One-Off, Monthly, Quarterly, Annually, etc.):

.....

Proposed mechanisms to secure the data being accessed:

If applicable, what systems are used to access the PID for Secondary Use Purposes?:

Service Manager Details

Service Manager Name:.....

Email Address:..... Contact Number:.....

Department:..... Directorate:.....

Service Manager Signature:..... Date:.....

CALDICOTT GUARDIAN USE ONLY

Caldicott Guardian Approval:

Name (Print):

Position:

Signature:..... Date:.....

Appendix 2 - Caldicott Principles

What is Caldicott?

The term Caldicott refers to a review commissioned by the Chief Medical Officer. A review committee, under the chairmanship of Dame Fiona Caldicott, investigated ways in which patient information is used in the NHS.

The review committee also made a number of recommendations aimed at improving the way the NHS handles and protects patient information.

What is a Caldicott Guardian?

A Caldicott Guardian is a senior person responsible for protecting the confidentiality of patient and service-user information and enabling appropriate information-sharing.

The Guardian plays a key role in ensuring that the PCT satisfies the highest practical standards for handling patient identifiable information.

Acting as the 'conscience' of an organisation, the Guardian actively supports work to facilitate and enable information sharing and advise on options for lawful and ethical processing of information as required.

The Caldicott Guardian also has a strategic role, which involves representing and championing Information Governance requirements and issues at Board level.

These recommendations are summarised by the Six Caldicott Principles:

Principle 1 – Justify the purpose(s)

Justify the purpose. Every proposed use or transfer of patient identifiable information within or from an organisation should be clearly defined and scrutinised, with continuing uses regularly reviewed, by an appropriate guardian.

Principle 2 – Do not use personally identifiable information unless it is absolutely necessary.

Don't use patient identifiable information unless it is absolutely necessary. Patient identifiable information items should not be included unless it is essential for the specified purpose(s) of that data flow. The need for patients to be identified should be considered at each stage.

Principle 3 – Use the minimum personally identifiable information.

Use the minimum necessary patient identifiable information. Where the use of patient identifiable information is considered essential, the inclusion of each item of information should be considered and justified so that the minimum amount of identifiable information is transferred or accessible as necessary.

Principle 4 – Access to personally identifiable information should be on a strict need to know basis.

Access to patient identifiable information should be on a strict 'need to know' basis. Only those individuals who need access to patient identifiable information should have access to it, and they should only have access to the specific items they need to see. This may mean introducing access controls or splitting information flows (where one flow is used for several purposes).

Principle 5 – Everyone should be aware of their responsibilities.

Everyone with access to patient identifiable information should be aware of their responsibilities. Action should be taken to ensure that those handling patient identifiable information - clinical and non clinical staff – are made fully aware of their responsibilities and obligations to respect patient confidentiality.

Principle 6 – Understand and comply with the law.

Understand and comply with the law. Every use of patient identifiable information must be lawful. Someone in each organisation handling patient information should be responsible for ensuring that the organisation complies with legal requirements.

Appendix 3 - 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 / Head of Information
Directorate	Finance and Performance
Name of Document / Policy / Strategy / Procedure	Pseudonymisation (De-identification) Policy
Document Status	New Document <input checked="" type="checkbox"/> Existing Document <input type="checkbox"/>
Associated Policies, Strategies or Procedures	<ul style="list-style-type: none"> • Acceptable Use of E-mail Policy • Information Governance Policy • Safe Haven Policy • Bulk Transfer of (Electronic) Patient Records Policy • Confidentiality and Data Protection Policy • NHS Confidentiality Code of Practice • Performance and Conduct Policy • Serious Incident 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	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 4 - Audit Tool For The Pseudonymisation (De-identification) 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 Process for granting access to PID for Secondary Use Purposes?	Yes / No
Do you understand the need to use Safe Haven Procedures?	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 6 - Policy Ratification and Publication

Policy Title (including version)	Date
Pseudonymisation (De-identification) Policy 1.0	23/03/2011
Reason for Submission (Please Tick)	
Scheduled Review <input type="checkbox"/>	New Policy <input checked="" type="checkbox"/>
Urgent Amendments <input type="checkbox"/> (Please specify)	Other <input type="checkbox"/>
Purpose of Policy	
This policy outlines the PCT's approach to Pseudonymisation (de-identification) of Patient Identifiable Data for Secondary Use Purposes.	
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"> Information Governance & Data Protection Officer Head of Information Acting Head of Governance Business Systems Manager 	
New Policy: (Please reference sources of Best Practice used, and list applicable legislation)	
Sources of Best Practice: <ul style="list-style-type: none"> Connecting for Health Guidance (http://www.connectingforhealth.nhs.uk/systemsandservices/sus/delivery/pseudo) 	
Applicable Legislation and Codes: <ul style="list-style-type: none"> Data Protection Act 1998 Human Rights Act 1998 NHS: Confidentiality: NHS Code of Conduct 	
Reviewed/Amended Policy: (Please provide full details of changes made, reference sources of Best Practice used, and list applicable legislation)	
N/A	
Policy Equality Impact assessed	
TBC	
Policy Approval	
Name:	Chair of ICT & IG Programme Group
Signature:	Mark Easton
Date:	23/03/2011
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	