

## *Safe Haven Policy*

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

**To be read with:**

- Confidentiality and Data Protection Policy
- London Borough of Brent Overarching Inter-agency Information Sharing Protocol
- Acceptable Use of Email Policy
- Notification of New Flow of Person Identifiable Data Form
- Bulk Transfer of (Electronic) Patient Records Policy
- Records Management Strategy/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
0.1	Initial Draft.	N/A	Information Governance & Data Protection Officer	16/01/2009
1.0	Approved		Information Governance & Data Protection Officer	05/06/2009
1.1	Added Disciplinary and Monitoring and Reviewing Sections.  Added SMS / Texting section.  Reference made to Fraud.	Annual Review	Information Governance & Data Protection Officer	22/06/2010
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. Legislation and Guidance .....	4
5. Definitions .....	5
6. Responsibilities .....	5
7. Requirements .....	6
8. Sharing Information with other Organisations (Non NHS) .....	9
9. Disciplinary Procedures .....	9
10. Monitoring and Review .....	9
Appendix 1 – Fax .....	10
Appendix 2 – Post .....	11
Appendix 3 – Phone .....	12
Appendix 4 – Transporting .....	13
Appendix 5 – Example Fax Cover Sheet .....	14
Appendix 6 – New Flow of Person Identifiable Data Form .....	15
Appendix 7 – Registering for an NHSmail E-mail Account .....	17
Appendix 8 - Equality Impact Assessment Tool .....	20
Appendix 9 - Audit Tool For The Safe Haven Policy .....	22
Appendix 10 - Assurance Form .....	23
Appendix 11 - Policy Ratification and Publication .....	24

## 1. Introduction

- 1.1 Where other Trust locations, other Trusts or other agencies want to send personal information to a Trust department, they should be confident that they are being sent to a location which ensures the security of the data.

## 2. Purpose

- 2.1 All NHS organisations require Safe Haven procedures to maintain the privacy and confidentiality of the personal information held. The implementation of these procedures facilitates compliance with the legal requirements placed upon the organisation, especially concerning sensitive information (e.g. people's medical condition).

## 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 This policy provides:
- The legislation and guidance which dictates the need for a Safe Haven.
  - A definition of the term Safe Haven.
  - When a Safe Haven is required.
  - The necessary procedures and requirements that are needed to implement a Safe Haven.
  - Rules for different kinds of Safe Haven.
  - Who can have access and to who you can disclose.

## 4. Legislation and Guidance

- 4.1 A number of Acts and guidance dictates the need for Safe Haven arrangements to be set in place, they include:

**Data Protection Act 1998** (Principle 7): *“Appropriate technical and organisational measures shall be taken to make personal data secure”.*

**NHS Code of Practice: Confidentiality** Annex A1 Protect patient Information *“Care must be taken, particularly with confidential clinical information, to ensure that the means of transferring from one location to another are secure as they can be”.*

- 4.2 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.

## **5. Definitions**

### **5.1 Safe Haven**

The term Safe Haven is a location (or in some cases a piece of equipment) situated on Trust premises where arrangements and procedures are in place to ensure person-identifiable information can be held, received and communicated securely.

### **5.2 Personal Information**

Personal information is information which can identify a person – in which the person is the focus of the information and which links that individual to details which would be regarded as private. e.g. name and private address, name and home telephone number, etc.

### **5.3 Sensitive Personal Information**

Sensitive personal information is where the personal information contains details of that person's:

- Health or physical condition
- Sexual life
- Ethnic origin
- Religious beliefs
- Political views
- Criminal convictions

For this type of information even more stringent measures should be employed to ensure that the data remains secure.

### **5.4 Where Safe Haven Procedures Should Be In Place**

Safe haven procedures should be in place in any location where large amounts of personal information is being received held or communicated especially where the personal information is of a sensitive nature. There should be at least one area designated as a Safe Haven at each of the Trust sites.

## **6. Responsibilities**

### **6.1 Caldicott Guardian**

The appointed Caldicott Guardian for the Trust must approve all procedures that relate to the use of patient information.

### **6.2 Information Governance & Data Protection Officer**

The Information Governance & Data Protection Officer is responsible for co-ordinating improvements in: data protection, the confidentiality code of conduct, and information security.

### **6.3 All Trust Staff**

All staff that process personal-identifiable information and Managers who have responsibilities for those staff.

## 7. Requirements

### 7.1 Location / Security Arrangements

- Safe Haven environments should be a room that is locked or accessible via a coded key pad known only to authorised staff or
- The office or workspace should be sited in such a way that only authorised staff can enter that location i.e. it is not an area which is readily accessible to any member of staff who work in the same building or office, or any visitors.
- If sited on the ground floor any windows should have locks on them.
- The room should conform to health and safety requirements in terms of fire, safety from flood, theft or environmental damage.
- Manual paper records contained person-identifiable information should be stored in locked cabinets.
- Computers should be not left on view or accessible to unauthorised staff and have a secure screen saver function and be switched off when not in use.
- Equipment such as Safe Haven fax machines should be turned off during out of office hours period.

### 7.2 Computers

- Access to any PC must be password protected, this must not be shared.
- Computer screens must not be left on view so members of the general public or staff who do not a justified need to view the information can see personal data. PCs or laptops not in use should be switched off or have a secure screen saver in use.
- Information should be held on the organisation's network servers, not stored on local hard drives. Departments should be aware of the high risk of storing information locally and take appropriate security measures.
- Personal information of a more sensitive nature should be sent over NHSmail with appropriate safeguards:
  - Clinical information is clearly marked.
  - Emails are sent to the right people.
  - Browsers are safely set up so that for example, passwords are not saved and temporary internet files are deleted on exit.
  - The receiver is ready to handle the information in the right way.
  - There is an audit trail to show who did what and when.
  - Information is not saved or copied into any PC or media that is "outside the NHS".

### **7.3 Fax**

Fax machines must only be used to transfer personal information where it is absolutely necessary to do so. You must remove patient identifiable data from any faxes unless you are faxing to a known secure and private area (Safe Haven). The following rules must apply:

- The fax is sent to a safe location where only staff that have a legitimate right to view the information can access it.
- The sender is certain that the correct person will receive it and that the fax number is correct.
- You notify the recipient when you are sending the fax and ask them to acknowledge receipt.
- Care is taken in dialling the correct number.
- Confidential faxes are not left lying around for unauthorised staff to see.
- Only the minimum amount of personal information should be sent, where possible the data should be anonymised or a unique identifier used.
- Faxes sent should include a front sheet, which contains a suitable confidentiality clause (Appendix 5).

### **7.4 Post**

- All sensitive records must be stored face down in public areas and not left unsupervised at any time.
- In coming mail should be opened away from public areas.
- Outgoing mail (both internal and external) should be sealed securely and marked private and confidential. See Appendix 2 for guidance.

### **7.5 Phone**

- Do not make telephone calls where you can be overheard (e.g. Reception)
- When telephone enquiries are received asking for disclosure of personal information, the caller should be asked to put their requests in writing where applicable. Where requests have to be dealt with more quickly, the following rules must be adhered to:
  - You must be sure that the disclosure is legally justified and the caller has a legal right to access that information.
  - Verify personal details.
  - Obtain and record enquiries telephone number.
  - If the caller is part of an organisation/company, you should obtain the main switchboard number of that organisation (via phone book or directory enquiries) and ring back.
  - Always provide the minimum amount of information that is necessary.
  - If in doubt, tell the caller you will ring back, where necessary consult a senior manager or the Trust's Caldicott Guardian.
  - All press enquiries for example should be directed to the Press and Communications Department.

See Appendix 3 for guidance.

### **7.6 Transporting**

See Appendix 4.

## 7.7

### **E-mail**

- Internal E-mail  
The transmission of Patient/Staff Identifiable Data or confidential business within NHS Brent (i.e. from joe.bloggs@brentpct.nhs.uk to john.doe@brentpct.nhs.uk) is permitted. However information should be kept to the absolute minimum, and should be transmitted in a file which can be password protected.
- E-mail within the NHS  
The transmission of Person Identifiable Data within the NHS must be done by using NHSmail. To obtain an NHSmail account go to [www.nhs.net](http://www.nhs.net) and register (Appendix 7). If there is a problem registering e.g. you are not registered with the Trust, contact Service Desk on Ext. 6676.
- Internet Email  
Under NO circumstances whatsoever should any type of patient, staff or business or confidential information be transmitted via Internet e-mail (e.g. Hotmail, Yahoo, G-Mail). Due to its insecure nature any information transmitted over the Internet should be considered to be in the public domain.
- For more detailed guidance on sending sensitive personal information electronically please also read the NHS Brent Acceptable Use of Email Policy.

## 7.7

### **Short Message Service (SMS) and Texting**

- Under NO circumstances whatsoever should any type of person identifiable patient or staff data be transmitted via SMS.
- Confidential business information should not be transmitted via SMS.

## 7.8

### **Bulk Transfer**

- Bulk transfers of confidential or Person Identifiable Data (50+ records) outside of the Trust must be authorised by the Trust's Caldicott Guardian and Information Governance and Data Protection Officer. To obtain authorisation your Service Manager must complete the form in Appendix 6.
- If you require guidance on securing data in transit please contact the Service Desk on 020 8795 6676 [servicedesk@brentpct.nhs.uk](mailto:servicedesk@brentpct.nhs.uk).

## **8. Sharing Information with other Organisations (Non NHS)**

- 8.1 Employees of the Trust authorised to disclose information to other organisations outside the NHS must seek an assurance that these organisations have a designated Safe Haven point for receiving personal information.
- 8.2 The Trust must be assured that these organisation are able to comply with the Safe Haven ethos and meet certain legislative and related guidance requirements:
- Data Protection Act 1998
  - Common Law Duty of Confidence
  - NHS Code of Practice: Confidentiality
- 8.3 Staff sharing personal information with other agencies should be aware of protocol agreements made with Brent Council, Central & North West London Mental Health Trust, The North West London Hospitals NHS Trust, Metropolitan Police Service, and London Fire Brigade.
- 8.4 If you are starting a new routine flow of Person Identifiable Data, then you must complete a Notification of New Flow of Person Identifiable Data Form, and return this to the Information Governance & Data Protection Officer (See Appendix 6).
- 8.5 Should a member of staff suspect that fraudulent activity is taking place regarding the disclosure of personal information, they should contact the Trust's Local Counter Fraud Specialist (LCFS). The LCFS for NHS Brent is Hannah Wenlock. Her contact details are:
- RSM Tenon  
45 Moorfields, London, EC2Y 9AE  
Tel: 020 7920 3200 or 07860 461 141  
Email: [hannah.wenlock@rsmtenon.com](mailto:hannah.wenlock@rsmtenon.com)

## **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 Untoward 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 9) will be used for monitoring purposes. The document Assurance Form (Appendix 10) will be used by Managers to document embedding of policies.

# Guidance

## Sharing Personal Information

### FAX

**If you are faxing to a known Safe Haven/Secure Fax, you do not need to follow any special instructions.**

**If not follow steps 1-6**

**6**  
If appropriate, request a report sheet to confirm that transmission was OK.

**5**  
Make sure your fax cover sheet states who the information is for, and mark it "Private and Confidential."

**1**  
Personal details should be faxed separately from clinical details, which must be accompanied by the NHS number

Do not fax personal or confidential information unless it is absolutely necessary.

**2**  
Telephone the recipient of the fax (or their representative) to let them know you are going to send confidential information.

**This guidance relates to Data Protection Principle 7 and Caldicott Principle 4**

**3**  
Ask the recipient to acknowledge receipt of the fax.

**4**  
Double check the fax number and use pre-programmed numbers wherever possible.

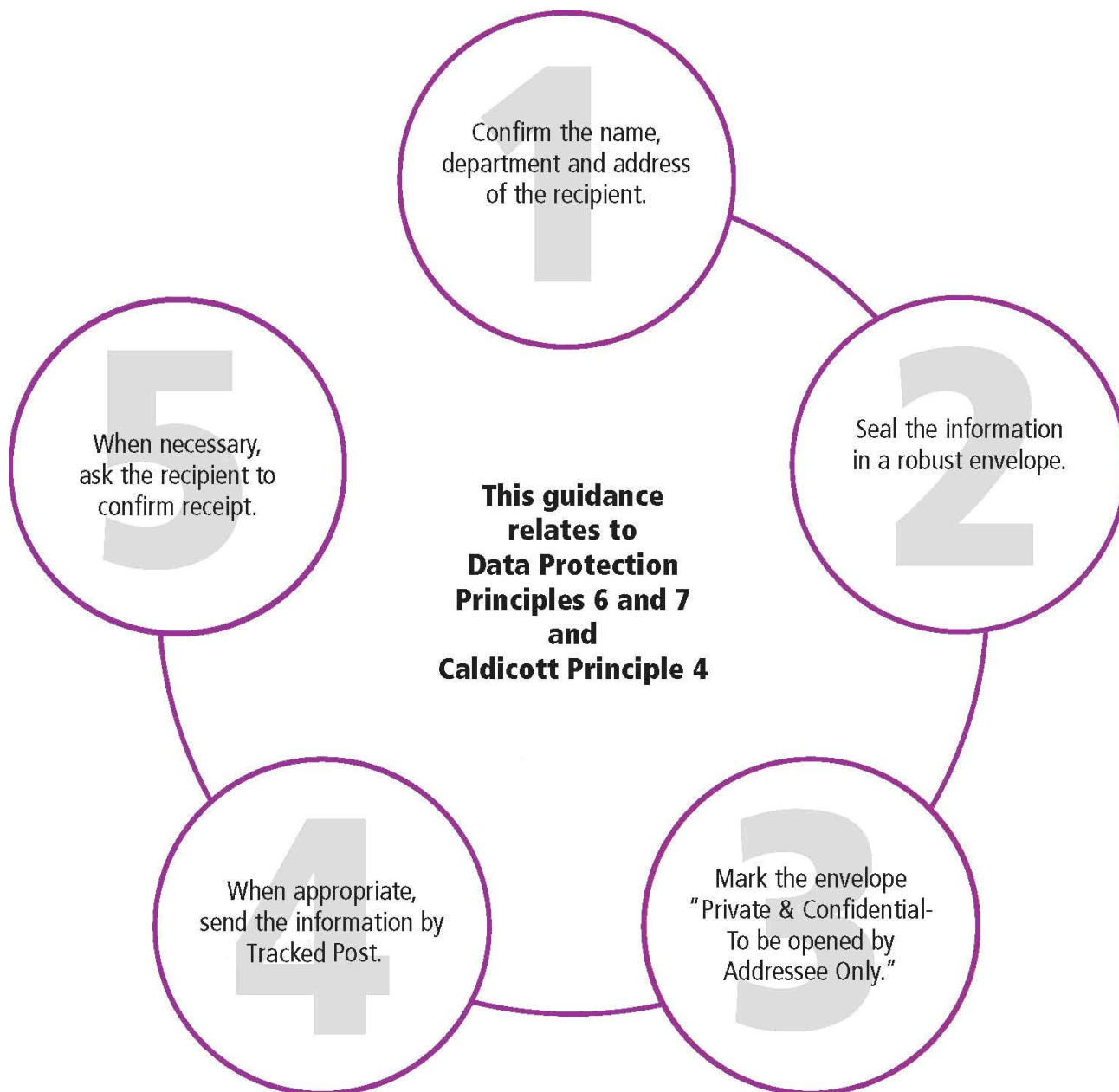


With acknowledgements to Surrey Health Community

# Guidance

## Sharing Personal Information

### POST

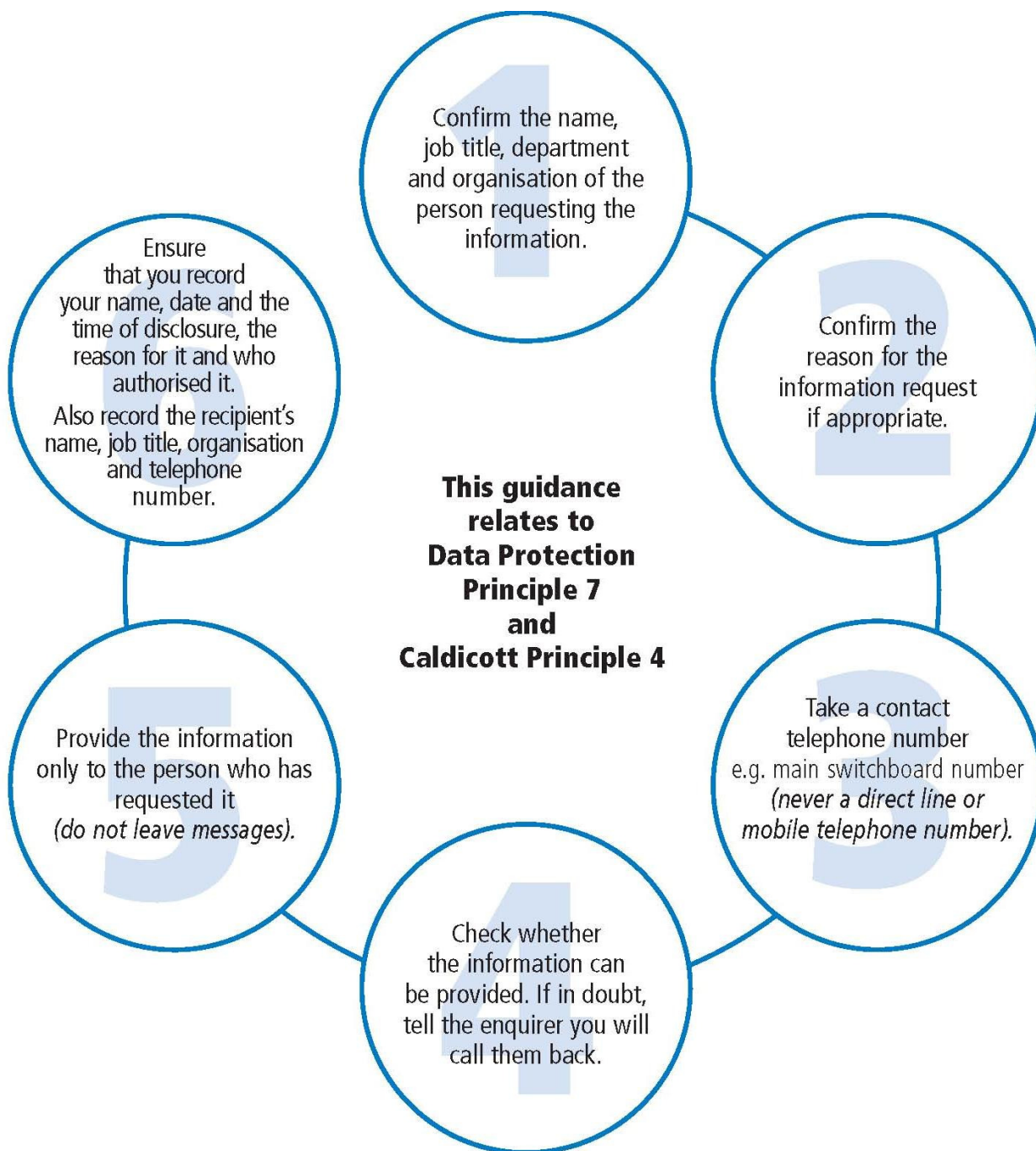


With acknowledgements to Surrey Health Community

# Guidance

## Sharing Personal Information

### PHONE



With acknowledgements to Surrey Health Community

# Guidance

## TRANSPORTING

### Personal Information





# Fax

Department  
Wembley Centre for Health & Care  
116 Chaplin Road  
Wembley  
HA0 4UZ

Tel: 020 8795 XXXX  
Fax: 020 8795 XXXX

<b>TO:</b>
<b>FAX NUMBER:</b>

<b>FROM:</b>
<b>FAX NUMBER:</b>

<b>No. of Pages:</b> (including this one)
--

<b>Date:</b>
--------------

<b>RE:</b>
------------

<b>CC:</b>
------------

<b>MESSAGE</b>
----------------

**CONFIDENTIALITY NOTICE** – *This fax is confidential and is intended only for the person to whom it is addressed. If you have received this fax in error, please immediately notify the sender on the number above and destroy all copies of the document received. If the reader of this fax is not the intended recipient, you are hereby notified that any distribution or copying of the fax is strictly prohibited.*

**IF YOU HAVE RECEIVED THIS FAX IN ERROR, PLEASE NOTIFY US IMMEDIATELY BY TELEPHONE – THANK YOU**

**If this message is incomplete or illegible, please telephone the number above.**

# Appendix 6 – New Flow of Person Identifiable Data Form

## Notification of New Flow of Person Identifiable Data Form

This Form is to be filled in by the relevant Service Manager when it is necessary to commence a new routine flow or Bulk Transfer (50+ Records) of Person Identifiable Data. This form should be sent to the Information Governance Officer for authorisation and risk assessment. You will shortly receive confirmation along with suggested method of data flow.

Service Area Details		
Service Manager Name:.....		
Email Address:.....	Contact Number:.....	
Department:.....	Directorate:.....	
Data Flow Details		
Data Description: .....		
.....		
.....		
Data contains the following details:		
Name <input type="checkbox"/>	D.o.B <input type="checkbox"/>	Gender <input type="checkbox"/>
Ethnicity <input type="checkbox"/>	Medical Details <input type="checkbox"/>	Address <input type="checkbox"/>
Other (please specify) .....		
.....		
.....		
Data Transfer/Flow Recipient or Source: .....		
.....		
.....		
Reason of Data Transfer/Flow: .....		
.....		
.....		
Format of Data Flow (i.e. electronic/paper based): .....		
.....		
.....		

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

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

Is it Bulk Data (details of more than 50 individuals)?

Do you consider data to be highly sensitive? (if so please provide reason):  
 .....  
 .....

Proposed mechanisms to secure the data in transit:  
 .....  
 .....

Proposed mechanisms to confirm receipt of the data:  
 .....  
 .....

---

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

Please return this form prior to commencement of new flow to:

Information Governance and Data Protection Officer  
 Talbot Offices  
 Wembley Centre for Health and Care  
 116 Chaplin Road  
 Wembley  
 HA0 4UZ

Any questions or problems please contact Information Governance and Data Protection Officer on 0208 795 7965

<b>INFORMATION GOVERNANCE USE ONLY</b>	
<b>Information Governance and Data Protection Officer Approval:</b>	
Signature:.....	Date:.....
<b>Caldicott Guardian Approval:</b>	
Signature:.....	Date:.....

## Appendix 7 – Registering for an NHSmail E-mail Account

### NHSmail

#### What is NHS Mail?

NHSmail is a secure national email and directory service for NHS staff in England and Scotland. It is provided free of charge and is available from any internet connected computer.

#### What are the benefits of NHSmail?

- NHSmail is a secure email service - this means that it is the only email service that can be used for exchanging confidential patient information.
- You can access your email from any computer that is connected to the Internet, at home or at work, wherever you are.
- Your email address with NHSmail will not change, even if your organisation does.
- You can send fax and SMS messages direct from NHSmail.
- NHSmail contains the NHS Directory, giving the contact details for all staff within the NHS.
- You can share mail and calendar folders with colleagues; for example, enabling a PA to manage your diary or sharing email within a team.
- A helpdesk is available 24 hours a day, 7 days a week.
- It is the only approved email system allowing the secure exchange of patient identifiable or clinical data information, and is endorsed by the following organisations:
  - The Royal College of Nursing
  - British Medical Association
  - The Chartered Society of Physiotherapy



## How Do I Register for an NHSmail e-mail account?

1. To sign up for your free NHSmail email address go to <http://www.nhs.net> and click on

 Register here

(Please note, you must use an NHSnet/N3 connected computer to register.)

2. Enter in your 'First Name' and 'Last Name', and click on

 Search

Click on your name.

3. Ensure that you have selected the correct person – Check the organisation assigned to your name. Click on

 Next

4. Read and Accept the "Acceptable Use Policy" by checking



Then click on

 Next

5. Choose an e-mail address by clicking on



Then click on

 Next

6. Complete the on screen instructions by providing 'Security Questions' and 'Security Answers'.

Then click on

 Next

7. Complete the Registration by checking your details and clicking on

 Finish

## Help

### NHS Brent IT Helpdesk

If when registering you are unable to find your name, please contact the IT Helpdesk.

[ServiceDesk@brentpct.nhs.uk](mailto:ServiceDesk@brentpct.nhs.uk)

0208 795 6676

### NHSmail National Helpdesk

NHSmail has a national helpdesk which is available 24 hours a day, 7 day a week, 365 days a year on 08453 0 08453 or email [helpdesk@nhs.net](mailto:helpdesk@nhs.net)

## Appendix 8 - Equality Impact Assessment Tool

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

### Summary

<b>Document Author</b>	Information Governance & Data Protection Officer
<b>Directorate</b>	Finance and Performance
<b>Name of Document / Policy / Strategy / Procedure</b>	Safe Haven Policy
<b>Document Status</b>	New Document <input type="checkbox"/> Existing Document <input checked="" type="checkbox"/>
<b>Associated Policies, Strategies or Procedures</b>	<ul style="list-style-type: none"> <li>Confidentiality and Data Protection Policy</li> <li>London Borough of Brent Overarching Inter-agency Information Sharing Protocol</li> <li>Acceptable Use of Email Policy</li> <li>Notification of New Flow of Person Identifiable Data Form</li> <li>Bulk Transfer of (Electronic) Patient Records Policy</li> <li>Records Management Strategy/Policy</li> </ul>
<b>Date</b>	

### 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 9 - Audit Tool For The Safe Haven 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 11 - Policy Ratification and Publication

Policy Title (including version)		Date
Safe Haven 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 Safe Haven procedures and provides guidance for staff to maintain the privacy and confidentiality of the personal information the PCT holds.		
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"> <li>• Head of ICT</li> <li>• Business Systems Manager</li> <li>• Information Governance &amp; Data Protection Officer</li> <li>• Head of Information (NHS Brent)</li> <li>• Head of Governance (BCS)</li> </ul>		
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"> <li>• Model Safe Haven Policy available on CfH IG Toolkit KnowledgeBase.</li> <li>• Policy Development Policy.</li> <li>• Department of Health Informatics Directorate Guidance: Short Message Service (SMS) &amp; Texting.</li> <li>• RMS Tenon LCFS Proactive Report Information Security Policies recommendations.</li> </ul> Amendments: <ul style="list-style-type: none"> <li>• Policy Development Policy format.</li> <li>• SMS Texting section added.</li> <li>• Disciplinary and monitoring and review sections added.</li> <li>• Reference made to Fraud</li> </ul>		
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		