Leicestershire County and Rutland NHS
Primary Care Trust

POLICY DOCUMENT

Transferring Patient Identifiable Information Policy

Approved by:	TRUST BOARD
On:	December 2007
Review Date:	December 2009
Directorate responsible for Review:	NURSING & QUALITY
Policy Number:	NQ020
Signed by:	Mrs Anna Barrett Director of Nursing & Quality

Equality Impact Assessment Tool

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

		Yes/No	Comments
1.	**Does the policy/guidance affect one group less or more favourably than another on the basis of:**		
	• Race	No	
	• Ethnic origins (including gypsies and travellers)	No	
	• Nationality	No	
	• Gender	No	
	• Culture	No	
	• Religion or belief	No	
	• Sexual orientation including lesbian, gay and bisexual people	No	
	• Age	No	
2.	**Is there any evidence that some groups are affected differently?**	No	
3.	**If you have identified potential discrimination, are any exceptions valid, legal and/or justifiable?**	No	
4.	**Is the impact of the policy/guidance likely to be negative?**	No	
5.	**If so can the impact be avoided?**	N/A	
6.	**What alternatives are there to achieving the policy/guidance without the impact?**	N/A	
7.	**Can we reduce the impact by taking different action?**	N/A	

If you have identified a potential discriminatory impact of this procedural document, please refer it to the Policy Administrator, 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 Policy Administrator.

Transferring Patient Identifiable Information Policy

VERSION CONTROL

First Version	Date	Amendment
V1	Oct 07	First Version

Contents

Paragraph **Page**

Appendices

Transferring Patient Identifiable Information Policy

1. INTRODUCTION

1.1 Introduction

1.1.1 In this age of instant communications it has become commonplace to use faxes and e-mail to transmit information. Unfortunately, these electronic systems have many vulnerabilities, which could result in the wrong person accessing potentially sensitive information. The same principles of handling information should also apply to written hard copy and portable electronic media such as CD's and Memory sticks. If the document contains personal information, which could identify a patient we all have a duty of confidentiality to recognise and manage these vulnerabilities.

1.2 Scope of Policy/Policy Statement

1.2.1**Scope** – This Policy is concerned only with the transferring of personal identifiable information as defined by the Data Protection Act 1998, the Caldicott Principles and NHS Information Governance Toolkit

1.2.2 **Policy Statement** – This policy applies to those members of staff that are directly employed by the PCT and for whom the PCT has legal responsibility. However, the PCT recognises that primary care practitioners are also part of the organisation and as such offers this policy for use by them to adapt to their own practices and organisations as appropriate. The contact for the policy is available to order help and support to primary care practitioners who wish to use and implement the policy.

1.3 Related Policies

- Information Security Policy
- E-mail and Internet Access and Monitoring Policy
- Confidentiality Code of Conduct
- Confidentiality of Patient Information Policy
- Policy for the reporting and management of Incidents/Serious and Untoward Incident Policy
- Risk Management Strategy
- Caldicott Approval Procedure

1.4 Definitions

1.4.1 **Safe Haven –** A 'Safe Haven' is a term used to describe an area where appropriate controls have been put into place to ensure that patient identifiable information is used with the appropriate levels of protection and security:

- Do not allow unauthorised people into areas where confidential information is kept unless supervised. Check peoples ID badges.
- Take measures to prevent casual scanning of information.
- Where possible store identifiable information in a locked draw/filing cabinet.
- Do not leave medical notes or personal information unattended at any time.
- Appropriately dispose of information that is no longer required (e.g. post it notes, and messages that do not require to be retained for any reason).

1.4.2 **Patient identifiable information** – This can be defined as individual identifying details such as patient name, address, and post code, date of birth, sex and NHS number. A combination of any two or more of these details are enough to be classed as identifying a patient according to the Department of Health Caldicott Committee's report on the review of patient identifiable information.

1.4.3 **Maximum baseline information** – An identifying code such as NHS number is meaningless unless the recipient has the decode information. Caldicott recommends the reduction of data down to NHS number only. Since the NHS number code is not universally available at this time it is acceptable to use a combination of the following:

- A code common to both parties (NHS number, hospital number or equivalent)
- Correlating a piece of information to positively identify the data subject e.g. an element of the date of birth or the first three letters of the postcode.
- A patient's name should only be used as an identifier in those circumstances where there are no other common items between the parties.

1.4.4 Address should not be transferred unless critical to the purpose of the transmission.

1.5 Key Messages

1.5.1 It is imperative that the utmost care is exercised when transferring patient identifiable information. To this end the use of written documents (including the use of white boards) as well as fax machines and e-mail should be used with care. When internal courier post or public mail is used, it is essential to confirm that the addressee details are correct. The basic rule is that in all circumstances where patient identifiable data is shared, by whatever method, the items transferred should be restricted to a minimum. Only those essential items of information should be included. Other items should be omitted or blocked before transmission.

1.6 Aim of this document

1.6.1 This document provides principles and procedures for avoiding accidental disclosure of sensitive information when the use of written documents (postal service), e-mail or fax may be acceptable, and to outline reasonable precautions that can be taken in those circumstances.

1.6.2 The policy applies to the following types of communication:

- Facsimile
- Internal and External Mail
- White Boards
- Telephones
- Answer Phone/Voice Mail
- Face to Face requests for information

1.6.3 The policy should be used in conjunction with the Trust's Confidentiality Code of Conduct and Records Management Policy which discusses how records should be used and transported.

2. Accountability Arrangements

2.1 Staff Roles and Responsibilities

2.1.1 **Chief Executive** – Has ultimate responsibility for security and patient confidentiality at Trust Level.

2.1.2 **Caldicott Guardian** – As recommended by the Caldicott committee, Leicestershire County and Rutland Primary Care Trust (hereafter identified within the document as the Trust) has appointed a Caldicott Guardian to take the lead in patient confidentiality issues. Where active advice is needed, the Cladicott Guardian should be the point of contact (see Trusts Caldicott Approval Procedure).

2.1.3 **Information Governance Manager** – Responsible for managing and introducing Trust guidance/policy and supporting staff/patients

2.1.4 **Line Managers** – Responsible for ensuring that all staff members who have the responsibility for transferring patient identifiable information use the procedures as agreed in this policy document.

3. Legal/Statutory obligations

3.1 All NHS organisations

3.1.1 All NHS organisations are under a legal, moral and professional obligation to ensure the confidentiality of personal data

3.2 Data Protection

3.2.1 The Data Protection Act 1998 also requires organisations to ensure that:

- Appropriate security measures are taken against unauthorised access to, or alteration, disclosure or destruction of, personal data
- Disclosure of information or data by transmission, dissemination or otherwise making available is included in the security measures.
- Organisations must implement security measures to restrict the transfer and holding of personal data.

3.3 Government recommendations

3.3.1 The Caldicott Report on the transfer of patient identifiable information, published in December 1997, made sixteen recommendations to be implemented by NHS organisations. The report recommends that trusts develop a Safe Haven policy for the secure transfer of patient identifiable information via fax. It also recommends that the NHS number should be substituted for patient identifiable data wherever possible and that where patient data is transferred it should be reduced to the minimum required for the purpose.

3.4 Professional codes

3.4.1 The General Medical Council’s web page “Guidance on Good Medical Practice”, contains guidance for health professionals. There is a link to “guidance” which includes a further link to a section on confidentiality. Section 4 “Protection patient information” states that “When you are responsible for confidential information you must make sure that the information is effectively protected against improper disclosure when it is disposed of, stored, transmitted or received”

3.5 Information Governance Toolkit

3.5.1 The Toolkit is a set of objectives that all NHS organisations are required to adhere to, promoting best practice within information governance. The Toolkit defines levels of compliance to which organisations are expected to achieve and maintain.

4. Facsimile (Safe Haven fax machines)

4.1 Only Fax machines which are located in a designated ‘Safe Haven’ environment, where confidential information can be disclosed or accepted on transfer from organisation to organisation are to be used for this purpose.

4.2 Consider the **Caldicott Principles** prior to faxing the requested information:

- Use and transfer of such information will only take place where the purpose is fully justified
- Use and transfer will only occur when absolutely necessary
- Use of the minimum required – where possible, all data should be anonymised
- Access should strictly be on a “need to know” basis
- Everyone must understand his or her responsibilities
- Understand and comply with the law

4.3 All staff are to take responsibility for sending confidential information via fax machines by:

- Contacting the relevant person/Department before sending the fax, to ensure they are available to receive the information
- Acknowledging receipt of information upon receipt
- Ensuring that you are using the Trusts Fax cover front sheet
- Double checking the fax/telephone number before you press the “send” button.
- Requesting a report sheet to confirm safe and correct transmission
- Awaiting acknowledgement from recipient or making a separate telephone call to the recipient to confirm receipt, especially when sending information outside of the Trust.
- Clearing the fax machines memory if copies are stored to its memory

4.4 Each fax machine should have a nominated person responsible for the equipment who should also ensure that staff are aware of this policy and are competent using fax. This person will be referred to as the ‘Safe Haven Guardian’. The guardian along with the details of their designated fax machine, is to be notified to the Information Governance Manager and Records Advisor, who will maintain the register. Any changes of personnel/equipment should also be noted.

4.5 Wherever possible clinical information should be faxed using the minimum amount of patient identifiable information to minimise any possible risks. The NHS number should be used as the primary source of identification.

4.6 Fax machines used to transmit patient information should be sited in a secure environment. Access should be limited to those people authorised by the Safe Haven Guardian in the department that the fax serves.

4.7 All incoming messages containing confidential information should be handled accordingly. **No printouts should be left unattended at the fax machine or in the print tray.**

4.7 All Safe Haven faxes that are sent out from within the Trust must be sent with the appropriate front sheet (Appendix A) as the first page. All the details on the front sheet must be completed. **No confirmation printouts should be left on the fax machine or in the print tray.**

4.8 Frequently used numbers should be programmed into the fax machines memory facility if there is one which will reduce the risk of dialling incorrect fax numbers.

5. Post

5.1 Incoming mail is to be opened away from public areas and by the addressee or designated person only.

5.2 Envelopes containing confidential information should be clearly marked ‘Confidential’ and may be opened by any staff member who works within the appropriate area and who has a ‘need to know’. Where information needs to be restricted to a named individual, for example staff information, the envelope should be addressed ‘Private and Confidential’.

5.2.1 Sending Mail to Patients

Post that it sent to patients should be addressed clearly and marked private and confidential. The patient’s name and correct address must be stated. This must be sent to the patient via Recorded Delivery.

5.2.2 Sending Mail to another staff member or to another party

All mail must be addressed clearly and adequately by ensuring that the recipients name is stated, their job title and the address where the correspondence is being sent.

5.2.3 Sending Mail to a Clinical/Admin team

If you are sending mail to a team/department where it is appropriate for it to be opened by any member of the team, there is no requirement to state an individual's name. Correspondence should be addressed with the job role/function and the department name.

5.3 When sending out information in the post where the recipient might not be clear as to the identity of the originator, staff should ensure that either a compliment slip is included or that the enclosure clearly states the name, title and contact details of the sender.

5.4 Where available internal courier services are to be used when sending information around the Leicestershire and Rutland Health Community.

5.5 Envelopes must be sealed, but staples should not be used as they are a health and safety risk.

5.6 It is good practice to use double envelopes for particularly sensitive internal mail and the use of tamper proof envelopes for health records.

6. E-mail and Computer Use

6.1 In relation to sending any personal information via e-mail please refer to the Trusts separate E-mail and Internet Access and Monitoring Policy. Only NHS Mail email accounts ending in nhs.net and nhs.uk, and which is used between both the sender and recipient should be used to email any patient identifiable information. **This is currently not available to LCRPCT staff, however means of secure transmission for patient identifiable information via email is being explored by Leicestershire Health Informatics Service.**

Patient identifiable information should not currently be sent via email.

7. Telephone Guidance

7.1 General guidance

Wherever possible, information should be passed as part of an agreed process with known individuals, where the need and authority to share has already been established. Where this is not possible the guidance below should be adhered to:

7.1.1 Answering the telephone

- Clearly state your name, status and department
- Ask who is calling
- Ascertain the nature of the call

7.1.2 What information can you give relatives/next of kin?

- Check the identity of the caller and the patients full name whom they are enquiring about.
- Think about the information you may be giving, clinical details should not be given out without the consent of the person concerned, the patient may not want this information being passed on to other relatives.
- Consent should be gained from patients regarding who they are happy for staff to discuss their health matters with. If this is not possible owing to the patient's condition, staff members will be required to make their own judgement and may be required to justify their decision.
- If you are in any doubt take the callers contact number and phone them back to a main recognised Department/switchboard and ask for them either by name/extension number.
- If you are unsure of the callers identity and do not know how to proceed, talk to your manager or contact the Information Governance Manager and Records Advisor.

7.1.3 **What information can you give to the police?**

- Refer to the Trust's Confidentiality of Patient Information Policy.
- Discuss with your manager
- If you require assistance contact the Information Governance Manager and Records Advisor

7.1.4 **What information can you give the Media/Press?**

All calls from the Media or Press should be passed on to the Communications Department and the Trust communication policies should at all times be adhered with. Under no circumstances should you give out any personal information without permission.

7.1.5 **What information can you give to other NHS staff?**

- Check the identity of the member of staff – their name, department and the nature of the enquiry.
- Request their telephone number and call them back
- If there is a genuine need for clinical information to be released be aware of others who may be listening
- If you are unsure of the callers identity and do not know how to proceed, talk to your line manager or contact the Information Governance Manager.

7.1.6 **What information can you give to the patient's employers?**

No information can be given to the patients employers without explicit consent of the patient/data subject. Refer any such enquiries to the HR Department.

8. Answer Phone/Voice Mail Messages

8.1 If you are required to contact a patient by telephone, it is best practice to gain consent from the patient in advance to establish whether they are happy for you to leave a message, if necessary. This consent and nay specific requirements are to be recorded in their health record.

8.2 If you are required to leave a message on a patients answer phone/voice mail without prior consent, for example the cancellation of an appointment at short notice, you are not to mention the fact that you are ringing from the Trust or leave any clinical information. The only information you are to leave is your name, telephone number and a brief message asking them to call you back.

8.3 Staff are not to leave messages for patients if there is any doubt regarding the validity of the telephone number.

8.4 The dangers of leaving messages are:

- Who might hear the message?
- Are you sure that you have telephoned the correct number?
- Will the recipient fully understand the content of the message?
- Can you be certain the message has been received by the patient?
- You may inadvertently breach patient confidentiality because the patient's friends or relatives may not know the patient is receiving health care.

9. White Boards

9.1 White boards and name boards above patients beds and in other patient areas should only state the patient's name (initials preferably), and if a patient insists that they do not want this information displayed in a visible public area you must respect their decision.

9.2 No other patient identifiable information should be put onto the whiteboards located in a general public area, for example address, date of birth or specific clinical details

9.3 If it is absolutely necessary to put clinical information onto a whiteboard not located in a public area, the information should be abbreviated or symbolised so as only health professionals can understand the information and not other members of staff that may come into the department.

9.4 Whiteboards used for clinical or patient information should only be used in areas which are restricted to staff only and cannot be viewed by patients or other members of the public.

10. Face to Face Requests for Patient Information

You may be asked the whereabouts of a patient e.g. if you are working on a reception area.

- Establish the fullest details of the patient as a means of establishing the authenticity of the enquirer.
- Ask the relationship of the enquirer to the patient
- Ask what department/ward they think the patient may be attending and ask them to take a seat for a moment
- Try to ascertain the whereabouts of the patient
- If you manage to locate the patient telephone the department and ask permission from the patient to send the enquirer/relative to that area if it is appropriate or pass the message on that they are here waiting.

11. Incident Reporting

11.1 An Information Security incident is defined as any event, which has resulted **or could have** resulted in:

- The disclosure of confidential information to any unauthorised individual
- The integrity of the system or data being put at risk
- The availability of the system or information being put at risk
- An adverse impact, for example:
  - embarrassment to the Trust/NHS
  - threat to personal safety or privacy
  - legal obligation or penalty
  - financial loss, or
  - disruption of activities

11.2 There are grades of seriousness, which can be applied to security incidents. The majority of security breaches are innocent and unintentional but staff should report any actual **or suspected** breaches of security or potential weaknesses in secure operation of any systems, including fax machines or e-mail.

11.3 Security incidents need to be reported through the PCT's Risk Management Process by completing an Incident form (IR1/IF1). Further information can be found in the Policy for the reporting and management of Incidents/Serious and Untoward Incident Policy.

12. Audit (faxes only)

12.1 A logging system should be set up and kept for future reference. All confidential faxes sent should be logged. The log should include the following details as a minimum:

- Senders name
- Senders contact details
- Date and time
- Recipient organisation
- Recipients name
- Recipients telephone number
- Printout from fax machine of transmission success
- A copy of the cover sheet, which should contain these details and would form the basis of a suitable system

12.2 If it is available, a printout will be requested periodically showing usage of the fax line. Printouts should be compared against the usage log to check errors. Anomalies should be followed up and corrective action taken where necessary. Should an anomaly represent a threat, or possible threat, to information security, the event should be reported to the Information Security Officer (via the HIS service desk) and to the PCT Information Governance Manager. The log should be subject to spot check by the Safe Haven Guardians and by the Information Governance Manager.

12.3 Appendix ? shows an example audit sheet whilst Appendices ? and ? show sample log sheets

13. Training, Communication and Review

13.1 Training

13.1.1 All staff should receive training in elements relevant to their role and scope of responsibility. The appropriate line managers will receive in-house training and then relay that training to staff. All training must be documented on staff personnel files. The training needs of individual members of staff will be identified through the PCT's annual appraisal process and the production of personal development plans.

13.1.2 New members of staff joining the PCT are required to attend Alfred Hill Induction Training which includes an Information Governance session covering an introduction to information security, confidentiality, data protection and records management.

13.2 Communication

13.2.1 Copies of this Policy will be made available to all staff via the Policy Files on the PCT's intranet.

13.2.2 All staff will be notified of a new or reviewed policy via the PCT News

13.2.3 This document will be included in the PCT Publication Scheme in compliance with the Freedom of Information Act 2000.

13.3 Review

13.3.1 This Policy will be reviewed every two years by the Information Governance Manager and Information Security Officer, or as and when significant changes make earlier review necessary.

14. Acknowledgements

This Policy has been developed and built on from the policies and procedures of the following organisations:

- Gloucester PCT – Safe Haven principles
- Devon PCT – Safe Haven Fax procedure
- East Surrey PCT – Guidance for sharing personal information by post
- Lincolnshire PCT – Safe Haven and Communication Policy
- Newcastle PCT – Transferring Patient Identifiable Information Policy

15. Contacts

- Caldicott Guardian based at LCRPCT HQ, Lakeside House, 1 Smith Way, Grove Park, Enderby, Leics. LE19 1SS
  Telephone: 0116 295 7572

- Information Governance Manager based at PCT North base Offices, Woodgate, Loughborough, Leics. LE11 2TZ
  Telephone: 01509 567722

- Information Security Officer based at Gwendolen House, Gwendolen Road, Leicester
  Telephone: 0116 295 2376

- IT Service Desk based at Health Informatics Service, Gwendolen House, Gwendolen Road, Leicester
  Telephone: 0116 295 3500

Appendix A

Name of local office
Address 1
Address 2
Address 3
Address 4
Leicestershire
Postcode

Tel: xxxx xxx xxxx
Fax: xxxx xxx xxxx
Direct dial: xxxx xxx xxxx
Minicom: xxxx xxx xxxx

Leicestershire County and Rutland NHS
Primary Care Trust

Fax

To:	[Click **here** and type name]	**From:**	[Click **here** and type name]
Fax:	[Click **here** and type fax number]	**Pages:**	[Click **here** and type # of pages]
Phone:	[Click **here** and type phone number]	**Date:**	12/12/2007
Re:	[Click **here** and type subject of fax]	**CC:**	[Click **here** and type name]

□ **Urgent** □ **For Review** □ **Please Comment** □ **Please Reply** □ **Please Recycle**

Title (This should summarise the content of your fax)
Insert the details of your memo here…

This Facsimile message is intended for the addressee only and is strictly confidential. If for any reason it has been received by you in error, we apologise and would be grateful if you would contact the sender on the above telephone number and destroy your copy. THANK YOU IN ANTICIPATION OF YOUR ASSISTANCE.

Appendix B

Transmission Procedure

When sending patient identifiable information please follow the procedure as outlined below:

- Check that you have the correct details of the Safe Haven fax you are transmitting to. You can get this information at http://nww.connectingforhealth.nhs.uk/nacs/publications/safehavens/shmain.pdf The details (contact person, telephone number and fax number) of each organisation are listed alphabetically

- The PCT's corporate fax cover sheet must be used and must clearly show who the message is intended for and contact details for the sender
  - ° It must be marked ***"Confidential and Urgent"***
  - ° The total number of pages that are being sent must be entered

- The message should also bear a notice to the following effect:
  - ° The information in this fax document is confidential and may be legally privileged
  - ° It is intended solely for the addressee
  - ° Access to this document by anyone else is unauthorised
  - ° If you are not the intended recipient, any disclosure, copying, distribution or any action taken or omitted to be taken in reliance on it is prohibited and may be unlawful
  - ° If this document is received by anyone other than the addressee, please contact the sender.

- Unless you are sending details to an unmanned (but securely positioned) fax machine for example, when sending Out of Hours reports to arrive before 9am to a GP practice, you should:
  - ° Contact the recipient to ensure they are available and to allow them to prepare to receive the fax within an agreed timescale
  - ° Request that the recipient contacts you to confirm receipt or none delivery

- Take great care when dialling the number; check a reliable and up-to-date source for the number. If the facility exists, double checking the ID returned by the fax to ensure to the best of your knowledge that it is the correct fax machine that is answering.

- Should a published fax number turn out to be incorrect, inform the Information Governance Manager on 01509 567722

- If anything appears wrong suspend the call immediately

- On completion retain the printed record of transmission and include it with a copy of the cover sheet (or the original if you do not require it any more). Give this to the Safe Haven Guardian for inclusion in the log.

Leicestershire County and Rutland **NHS**

Primary Care Trust

Appendix C

Fax Audit Checklist

Ensure that 10% or a minimum of 20 faxing practice/fax records are audited every three months.

1. **There is written guidance available detailing the action to be taken when faxing confidential information?**

   Yes □ No □

2. **Staff can demonstrate an awareness of the procedures to be taken when faxing confidential information?** (Interview staff members)

   Yes □ No □

3. **There is evidence that the sender dials the number and then rechecks the number against the intended recipient's number prior to pressing the "start" button and sending the information?** (observe staff faxing information or confirm the procedure with staff members during the interview)

   Yes □ No □

4. **There is evidence that a fax cover page containing the following information precedes every transmission?** (observe faxing practice or ensure a fax cover sheet is available containing the following information)

• Whom is the fax from	Yes □	No □
• Who the fax is to	Yes □	No □
• Dept name (if appropriate)	Yes □	No □
• Contact address	Yes □	No □
• Contact telephone number	Yes □	No □
• Contact fax number	Yes □	No □
• Date	Yes □	No □
• Total number of pages	Yes □	No □
• A disclaimer statement	Yes □	No □

5. **Evidence exists that all fax receipts are recorded in a fax log?**

   Yes □ No □

6. **If a fax has been sent to the wrong destination, is there evidence that the correct action was taken?**

   Yes □ No □

APPENDIX D

Incoming Fax Log (Example)

Fax Machine number ……………………………………………………………………………

Location ……………………………………………………………………………

Date	Time	Minimum identifier of person in message – i.e. NHS No	Senders Organisation	Senders Department	Senders Tel. No	Reason	Details	Received By
06/11/07	13.00	Xx123456xx	ABC Trust	Rehabilitation	0000 11233	Fall	Transfer	J Bloggs

Leicestershire County and Rutland NHS
Primary Care Trust

APPENDIX E

Outgoing Fax Log (Example)

Fax Machine number ……………………………………………………………………..

Location ……………………………………………………………………..

Date	Time	Minimum identifier of person in message – i.e. NHS No	Recipient organisation	Recipient department	Recipient Tel No.	Reason	Details	Sent By
06/11/07	13.00	Xx123456xx	ABC Trust	Rehabilitation	0000 112233	Fall	Transfer	J Bloggs