East Lancashire NHS

Primary Care Trusts

SAFE HAVEN POLICY

Produced by: BRIDGET HILTON & ROBERT IRWIN

Ratified:

Review date: DECEMBER 2008

THIS POLICY HAS BEEN APPROVED AS AN EAST LANCASHIRE PRIMARY CARE TRUST POLICY THROUGH THE INFORMATION GOVERNANCE GROUP

1. Introduction

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).

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 been sent to a location which ensured the security of the data.

2. The scope of this policy

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 who you can disclose to

3. Legislation and guidance

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. Definitions

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-indefinable information can be held, received and communicated securely.

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.

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.

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 e.g. patient-identifiable information. There should be at least area designated as a safe haven at each of the Trust sites.

5. Responsibilities for implementing the Safe Haven Policy

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

Information Governance Manager
The Information Governance based at the Primary Care Informatics Unit is responsible for co-ordinating improvements in: data protection, the confidentiality code of conduct, and information security. The manager is assisted by the **Information Governance Support Officer** who has responsibilities the three East Lancashire PCTs in data protection and confidentiality matters.

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

6. Requirements for safe havens

Location/security arrangements

- It 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 fax machines in the safe haven should have a code password and be turned off out of office hours.

Fax machines

Fax machines must only be used to transfer personal information where it is absolutely necessary to do so. The following rules must apply:

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

Communications by 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

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 device 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.
- All personal information sent by e-mail should be password protected.
- 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
    - Information sent by email will be safely stored and archived as well as being incorporated into patient records
    - There is an audit trail to show who did what and when
    - There are adequate fall back and fail-safe arrangements
    - Information is not saved or copied into any PC or media that is "outside the NHS"

Great care should be taken in sending personal information especially where the information may be of a clinical nature – it should be password protected and procedures undertaken to ensure that the correct person has received it.

Please also read the East Lancashire Primary Care Trusts Internet and E-mail policy for more guidance on sending of personal information electronically.

7. Sharing information with other organisations (Non NHS)

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.

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

Staff sharing personal information with other agencies should be aware of protocol agreements made with Blackburn and Darwen Primary Care Trust; Lancashire County Council; and Lancashire Constabulary.

8. Other relevant polices

Other policies that need to be read in conjunction with this policy are:

- **Records management:** storage, handling, retention and destruction of records
- **Confidentiality:** rules for the use, access to, and disclosure of records
- **Email and Internet :** guidance on content

9. Contacts and further information

Information Governance Manager
Primary Care Informatics Unit
Cobham House
Haslingden Road
Blackburn
BB1 2QH
01254 269300

The **Information Governance Support Officer** can also be contacted at the above address and telephone number immediately above.

Caldicott Guardians:

All three PCTs have Caldicott Guardians they can be contacted at the addresses below:

Burnley, Pendle and Rossendale PCT
31/33 Kenyon Road
Lomeshaye Estate
Nelson
BB9 5SZ
01282 619909

Blackburn with Darwen PCT
Guide Business Centre
School Lane
Blackburn
BB1 2QH
Tel: 01254 267000

Hyndburn and Ribble Valley PCT
Red Rose Court
Clayton Business Park
Clayton Le Moors
Accrington
BB5 5JR
01254 380400

Also consider the following websites

The Information Commissioner http://www.informationcommissioner.gov.uk/

NHS Code of Practice: Confidentiality http://www.dh.gov.uk/assetRoot/04/06/92/56/04069256.pdf