East London NHS
NHS Foundation Trust

Safe Haven Guidelines for Staff

Contents

1. Introduction

These guidelines are to ensure that the transfer of person identifiable information into and out of the Trust and within the Trust between departments and sites is as secure as possible. The guidelines cover all person identifiable information which may relate to patients, staff, service users, or third parties about whom we hold information.

All routine flows of personal identifiable information either in or out of departments should be recorded. The flows should be justified, in accordance with the Caldicott Principles, where they are not directly related to the care of service users. Safe receipt of person identifiable or sensitive data should be confirmed in all cases.

2. Definition of a Safe-haven

A safe haven is a location which is set up to receive and manage confidential information appropriately. It may be a post room, reception area or fax machine, or anywhere where messages may be taken and held before being passed onto the appropriate recipient.

3. Safe Haven Fax

A safe haven fax must be located where no unauthorised person can access it. In practice this means that the fax should be kept in a separately locked room or cupboard or should be protected from access by a password known only to the appropriate group using it.

3.1 Sending person identifiable information by Fax

1. Where person identifiable information data is to be sent by fax the sender should ensure that an appropriate fax header with a disclaimer is used.
2. Check that the fax is going to an appropriate safe haven fax.
3. Use the machine to confirm the fax was sent.
4. Ask the recipient to acknowledge receipt.
5. For service user information send the service user demographics separately to the clinical information.
6. Double check the number after it has been typed into the machine and before sending.

Do

- Do check and double check that you have typed the recipient's number correctly.
- Do use pre-programmed numbers where possible.
- Do use an ELFT cover sheet with instructions on it in case the fax is received by the wrong person.
- Do print a confirmation sheet for the transmission.
- Do follow Caldicott principles when sending person identifiable information so:
  - Do use the NHS number or other identifying number instead of name address and date of birth details if possible.
  - Do separate the clinical and demographic details if possible

Don't

- Don't send person identifiable information unless you can justify that it is necessary.
- Don't include person identifiable information details on the Cover sheet.

3.2 If a fax goes astray to an unintended recipient

1. Complete an incident form.
2. Ask the recipient to shred the information which they have received.
3. Make a note of the name and fax number of the unintended recipient.
4. Review the risk to the person whose personal information has been disclosed or lost.
5. Discuss immediately with your line manager and, where agreed, inform the person affected including any risk that you think has been caused.

6. If the person affected is a service user, make a note in the clinical record or ask an appropriate member of the care team to do so, stating how they were informed.
7. Explain to the person affected how they can make a complaint, should they wish to.

A list of safe haven faxes is available at

P:\IM&T Directorate\Information Governance\Send it Safe

4. Safe Haven Post

4.1 General

Much of the post received and sent by the Trust contains person identifiable information. Whilst the post is within the Trust's sites or management by subcontractors i.e. before it is passed to the Royal Mail, it should be held, transported securely and not left unattended. The wallets used in posting bulk person identifiable or sensitive data should be 'tamper proof', that is, it should be possible to tell if a seal has been broken in transit. Tamper proof wallets can be ordered from Postsafe Protective Mailing Supplies in the Office Depot Catalogue.

Where post has been opened on behalf of the intended recipient it must be stored where no-one can gain unauthorised access. Items marked Private and Confidential may only be opened by the addressee or by a person who has been specifically authorised by the addressee.

Each site in the Trust will designate a safe-haven point where mail which has been incorrectly addressed or the intended recipient is unclear can be opened and processed. This will normally be the site reception area unless otherwise agreed by the relevant Service Director. All items dealt with in such a way should be recorded including the eventual destination of the item of post. Where a member of staff has left the organisation any post to that person should be redirected to his/her line manager, who will decide what should be done with the item.

Small items of Person Identifiable data should: -

- Be placed in sealed envelopes and marked "Private and Confidential – Addressee only"
- Have a return address on the outside in the event of non delivery. If in doubt staff can use the Trust Post Office Box address

If undelivered please return to: P.O. Box 48792 London E1 6XZ

- Be clearly addressed preferably to a named person not just a department or ward

For large items of post and multiple records transfers see guidance on Bulk transfers below.

4.2 Transfer of person identifiable data or sensitive by post

Where the **bulk** transfer of person identifiable information is required special precautions should be taken.

- For any form of electronic removable media, encrypt all person identifiable or sensitive data in line with Trust encryption standards and use a padded envelope to protect the disk.

- Use **registered delivery** (next day delivery not via the ordinary mail) to protect the data from being lost.

- For paper based information, if the information cannot be transported by a member of staff, use **special delivery** or the Trust's approved courier service providers - TNT and Loomis.

- Do not send person identifiable data or sensitive data unaccompanied in taxis.

- In all cases, confirm receipt of the data by intended recipient

a) Internal transfers

Where the transfer is internal to the Trust i.e. between different sites and departments, transport via an individual member of staff where possible. The containers should be 'tamper evidenced', for instance it should be possible to tell if a seal has been broken in transit. (see transfer of casenotes).

All such transfers should be marked as confidential and should have a return address on the outside in the event of non delivery. They should be clearly addressed preferably to a named person not just a department or ward.

b) Transit of Casenotes

Formal track and trace procedures should be followed in line with the Trust's Health Record Keeping Policy. Where a service user is being transferred the casenotes should be transferred with the service user escort. Where it is necessary to transport the casenotes to another location within or outside the Trust, the casenotes should be placed in a sealed tamper proof wallet in order to reduce the risk of tampering with the records in transit.

Where the transfer of notes is carried out by a Trust employee they should follow Trust guidance on the transport of confidential material and the envelope should be addressed to a named responsible person (not a ward or

department). When transporting records individuals are tasked with ensuring their security and confidentiality.

4.3 If post goes astray or to an incorrect address

1. Complete an incident form.
2. Arrange for the unintended recipient to return the information or files to the Trust.
3. Review the risk to the person whose personal information has been disclosed or lost.
4. Discuss immediately with your line manager and, where agreed, inform the person affected, including any risk that you think has been caused.
5. If the person affected is a service user make a note in the clinical record or ask an appropriate member of the care team to do so, stating how they were informed of the loss of information
6. Explain to the person affected how they can make a complaint, should they wish to.