

Safe Haven Policy

Information Governance Committee Date Approved	14/03/08
Policy Consistency Group Date Approved	17/03/08
Date Ratified By Trust Board	26/03/08

Signature

Alex Fox

Reference Number
Version
Review Date
Lead Officer

Corp42
01
September 2008
Head of Integrated Governance

Corporate

CONTENTS

	Page No.
All about a Safe Haven	3-4
Do's and Don'ts	
➤ Information Storage	4-5
➤ Incoming and Outgoing Post	5-6
➤ Incoming and Outgoing Faxes	6
➤ Phones	7
➤ Shredding	7
Electronic Information	8-11
Safe Haven Fax Machines (Appendix 1)	12

This Safe Haven Guidance should be read in conjunction with:

- NHS Code of Practice for Confidentiality
- PCT Information Security and Confidentiality Policy
- PCT Records Management Policy

ANY INFORMATION SECURITY INCIDENTS SHOULD BE REPORTED IN ACCORDANCE WITH PCT PROCEDURES, AS QUICKLY AS POSSIBLE

What is a Safe Haven?

Safe Havens are needed to ensure the privacy and confidentiality of information and to meet legal requirements and Department of Health guidance.

All person identifiable information received by or sent from South Staffordshire PCT must be handled in compliance with South Staffs PCT Safe Haven procedures.

The use of written documents, fax machines, telephones, computer systems and Email should be governed by Safe Haven principles and procedures.

The utmost care must be exercised when transferring person identifiable information.

Transfer outside of Safe Haven must be minimised. When this is necessary, the amount of information transferred should be kept to a minimum.

Training

All staff must be trained in their responsibilities towards confidentiality. This is covered in induction, and ongoing training available through in-house training department.

What should it be used for?

A Safe Haven should safeguard patient identifiable information flowing to and from the organisation. Ideally, all information exchanged between NHS organisations should pass between Safe Haven points. This guidance also covers personal information about staff.

When information is disclosed by a designated Safe-Haven point to an equivalent point in another organisation, staff can be confident that agreed protocols will govern the use of information from that point on.

Scope of policy- Who should use a Safe Haven?

All staff who come across patient AND person identifiable information in any part of their work. e.g Finance team, admin staff as well as clinical teams..

What is patient identifiable information?

Examples of patient identifiable information are: (this list is not exhaustive)

- surname
- postcode
- initials
- sex

- forename
- address
- occupation
- NHS no
- sexuality
- date of birth
- National Insurance no.
- telephone no.
- local identifier (eg GP practice no.)
- ethnic group
- religion
- medical information

A patient can be identified from single items from the list above or combinations of two or more items (eg. postcode plus date of birth).

How is a Safe Haven created?

To create a 100% confidential environment the following need to be considered:

- access to person identifiable information
- information storage
- incoming and outgoing post
- incoming and outgoing faxes
- phones
- electronic information, including e mail; removable media and portable devices.
- shredding

Each of these should be managed in a way that its security is ensured.

Safe Haven Do's and Don'ts

Information storage

Do:

1. Ensure all patient /person identifiable information is stored in locked cabinets/rooms. These are designated Safe Havens for patient identifiable information.
2. When information needs to be removed for use, make a record of when it was removed and by whom, the person removing the information is then responsible for maintaining its confidentiality and returning it to the locked store (or their own "Safe Haven" locked cabinet) as quickly as possible.
3. Keep a note if any information is transferred so that it can be tracked if necessary.
4. Continuously assess whether information needs patient identifiers or whether it can be anonymised.
5. Nominate a person who is responsible for holding keys to the locked cabinets. This person will be responsible for the safe-keeping of the information stored within the cabinets.
6. Treat audio tapes awaiting text processing as confidential mail. Erase immediately after use.
7. Protect person identifiable data by encryption (or other SSPCT approved protection methods) and strong authentication.
8. Only transfer person identifiable data using secure and authorised PCTs and in accordance with SSPCT approved policies and procedures.

9. Store person identifiable data on SSPCT network server(s). Do not store on the local hard drive.
10. Only use registered and authorised laptops to process or hold person identifiable data. These must be configured to encrypt data and with anti virus/anti-malware software active on the device.
11. Carry out security checks on any incoming CDs/disks/tapes (e.g. virus checking)

Don't:

1. Copy person identifiable to removable media, unless it is absolutely necessary, it is properly authorised and is protected in accordance with SSPCT policies and procedures. (Note : where approved use only removable media owned by SSPCT. Personally owned media must not be used).
2. Leave any approved removable media containing person identifiable data accessible and on view, even in Safe Havens.
3. Label any approved removable media in any way that this would identify this media as holding person identifiable data.
4. Upload any incoming removable media (e.g. CDs/disks/tapes/USB drives, etc) from other organisations or other SSPCT areas until these have been security cleared (e.g. by virus checking).
5. Hold any person identifiable data on local drives. (Store only on protected, registered and approved SSPCT network servers).
6. Leave person identifiable data unattended at any time.
7. Leave person identifiable data in any area where it may be seen or looked at by unauthorised persons, even for short periods.
8. Leave files open when not in use.

Incoming and outgoing post

Do:

1. Deliver incoming post efficiently and quickly to the recipient. If the recipient is unavailable the designated deputy must take responsibility of that post.
2. If post is marked private and confidential to the named recipient, only they should open this (unless prior arrangements have been made).
3. Any confidential post not immediately given to the recipient must be locked away until they can receive it. The holder of the information is responsible for it until it is handed over.
4. Once the post has been passed over, it is the owner's responsibility to ensure the safe keeping of the information, using their own "Safe Haven" locked cabinet (see notes above on storage of information).
5. Make sure outgoing post is addressed to the correct recipient.
6. When sending post to another NHS organisation, use the internal mail service, if possible.
7. If highly sensitive (e.g complaints investigations) then call the recipient to ensure it has arrived safely (see Confidentiality Policy Feb 2008)

Don't:

1. Send any unencrypted data transfer by courier or post **UNLESS IT IS ESSENTIAL FOR PATIENT CARE**
2. Leave confidential post unattended in an open area.
3. Use removable media (i.e. computer disks, CD rom, DVD, flash memory, USB drives, portable hard drives, laptops) to transport person identifiable data. (If there is no other route then deliver personally or use recorded delivery and check that it has arrived). In both the above cases, approval and authorisation by SSPCT Caldicott Guardian and Information Security Officer is necessary before this method of transport can be used).
4. Never send person identifiable data to insecure locations.

Incoming and outgoing faxes

Fax machines must only be used to transfer person identifiable data where it is absolutely necessary.

Do:

1. Keep the fax machine in a secure location ie. in a locked room/cupboard out of any public area.
2. Deal with incoming faxes quickly and efficiently, and give to the recipient as soon as possible.
3. For outgoing faxes attach a cover sheet with a confidentiality statement (see below).
4. When sending outgoing faxes ensure the fax number is dialled correctly or use pre-installed fax numbers for safety. ALWAYS send confidential information to a Safe Haven fax or find a safer route of transfer.
5. It may be acceptable to use a recipient's fax which is not in a Safe Haven, but this should be for exceptional purposes only and ALWAYS telephone them to let them know the information is being faxed, ask them to wait by the fax machine and let you know when they have received the fax.
6. Where possible, use a linking identifier (eg. NHS number) rather than patient details. If patient identifiers need to be faxed then confirm the first part of the fax is in the right hands before faxing the remainder.
7. Request a report sheet that confirms your transmission is OK.
8. After sending confidential information erase the fax memory

Don't:

1. Send faxes to a destination where they won't be seen for some time (or outside office opening hours)
2. Leave the information unattended whilst it is being transmitted

Example wording for a fax cover sheet:

The information contained in this fax is STRICTLY CONFIDENTIAL and intended for the named recipient only. If you are not the named recipient you must not copy, distribute or disseminate this information, nor disclose its contents to any person. If you have received this fax in error, please notify the sender immediately.

Phones

Do:

1. Try not to disclose person identifiable data over the phone because of the risks involved (e.g. being overheard, inadvertent disclosure of confidential information, disclosing confidential information in an appropriate manner, etc).
2. Try to have phones away from the reception area. If this is not practical, take reasonable steps to protect a patient's confidentiality whilst speaking on the phone.
3. Ask questions over the telephone that require the patient to answer rather than giving them details which they need to confirm eg. try not to say 'is that Margaret Smith of 72 Town Road, Anytown?'. Instead, ask the patient who they are and where they live and do not repeat that information out loud.
4. If you receive a call from another health professional, confirm their identity and their reason for asking before giving out any confidential information.
5. If you have any doubt as to the identity of the caller, call them back using a published telephone number (rather than the one they quote).
6. Put callers on hold so that they can't hear other confidential conversations that may be going on in the office.
7. Before information is given out ensure that the enquirer has a legitimate right to have access to the information.
8. Ensure answer phones are located in a secure area and are only accessible by authorised personnel

Don't:

1. Repeat any confidential details that a patient gives you if others may hear them, eg. there is no need to mention forenames and surnames out loud in the same conversation.
2. Have the phone switched on to 'speaker' mode, turning a confidential call into a 'tannoy' message.
3. Assume permission if you are asked to give patient information to a relative – check with the patient or your manager first.
4. Leave messages containing confidential information on answering machines.

Shredding

Do:

1. Destroy confidential information in the correct way. Use the shredder for destruction of all confidential information.
2. Make sure everyone knows how to use the shredder and what type of information should be destroyed using it.
3. Make sure that where necessary records are kept for a legal length of time. (The Policy for Preservation, Retention and Destruction of Health Records and Other Corporate Records).
4. Treat surplus or spoiled photocopies of patient information as confidential waste.

Electronic information

The number of staff with access to person identifiable data should be kept to the minimum, on a strict need to know basis and consistent with job requirements.

(a) Access to Person Identifiable Data

Do:

1. Follow SSPCT Information Security policy and codes of practice when dealing with person identifiable data.
2. Use strong passwords with a minimum of 6 alpha numeric characters. (Avoid short and easily guessed passwords). Change passwords regularly. (This will be enforced by computer policy).
3. Use anti virus and malicious software protection on person identifiable data. (This will be enforced by computer policy).
4. Position screens so that they cannot be viewed by unauthorised persons.
5. Always exit applications and shut down fully at the end of the session.

Don't:

1. Disclose login or password details
2. Share login and passwords
3. Use passwords that relate to the system or information being accessed
4. Use passwords that are easy to guess. Don't write down passwords and then leave them where they can be seen by others.
5. Store or save passwords on the device or in a browser.
6. Leave PCs or laptops logged in and unattended, always log off or lock when not in use.
7. Position screens where they can be viewed by unauthorised persons.
8. Copy person identifiable data to any removable media or portable device unless this is authorised by SSPCT responsible officers (e.g. Caldicott Guardian).
9. Do not, where removable media or portable device is authorised to be taken off site, leave the media/device unattended at anytime (e.g. in cars or in any easily accessible area).

Note: Removable media is CD/DVD, floppy disk, zip drive, hard drives, back up storage unit, USB storage device, flash memory device, MP3/MP4 player or other media player, digital camera, mobile phone.

Note: Portable device is laptop, PDA.

(b) Transfer by Email

Email transmission over networks can have serious risks. Transfer of person identifiable data must be avoided unless essential to the delivery of healthcare. Where authorised Email has to be used, this must follow SSPCT Information Policy, guidance and good practice.

Do

- Person identifiable data can be sent between NHS mail accounts - but only when essential to service delivery and only where expressly authorised by SS PCT responsible officers (e.g. Caldicott Guardian) and only where all risk issues have been identified and suitably resolved. (The e mail will be encrypted automatically).
- Person identifiable data transferred by e mail must only be carried out using specifically registered, authorised and secure devices (PC; laptop) and only in accordance with SS PCT approved policies and procedures. (Personally owned devices must not be used).
- Suitable approved back up and fail safe facilities must be in place and operating satisfactorily before any allowed person identifiable data is transferred by e mail.
- Where transfer of person identifiable data by e mail is allowed; this must be sent as an encrypted attachment (and not in the body of the email).
- Where transfer of person identifiable data by e mail is allowed, a secure 'mechanism' must be in place to trace all person identifiable data transferred by e mail.
- The address of the recipient must first be confirmed, together with a test message also confirmed.
- The subject window of person identifiable data transferring by e mail must be identified as 'SAFE HAVEN'.
- E mail transferring person identifiable data must carry a SS PCT approved disclaimer for confidential information.
- The intended recipient must adhere to the principles of safe haven (i.e. to ensure that person identifiable data is only viewed by persons authorised to view such information)
- Person identifiable data sent to SS PCT by e mail must be virus checked before it is opened.
- Person identifiable data sent to SS PCT by e mail must only be stored on SS PCT registered secure network servers. (It must not be stored on PC's, laptops and other portable devices or removable media).

Don't

- Very sensitive information must not be sent by e mail
- Person identifiable data must not be sent by e mail unless it is encrypted to NHS approved standards and using software authorised and configured by SS PCT.

- Person identifiable data must not be sent to any non NHS mail account
- Person identifiable data must not be sent in the open body of the email. An encrypted attachment must be used.
- Person identifiable data must not be sent to shared or group e mail boxes (unless all those with access to the mail box have the necessary security authorisation and access).
- Person identifiable data must not be forwarded by email to any person or organisation that is not specifically authorised to receive and view that information.

(c) Laptops and Person Identified Data

- All laptops used for processing or holding person identifiable data must be uniquely identified and registered. Responsibility for keeping the laptop and information secure will be assigned to the responsible 'owner'.
- Laptops must not be transferred between 'owners' (users) unless authorised by SS PCT responsible officers and only in compliance with SS PCT approved procedures.
- Where processing/handling of person identifiable data is allowed on laptops, this must be authorised by relevant SS PCT Directors and the Caldicott Guardian.
- Sensitive data on laptops, where this is allowed (rarely) must be kept to the absolute minimum required for its effective use.
- All person identified data on laptops must be encrypted to NHS approved standards and using software authorised and configured by SS PCT.
- All registered and authorised laptops, permitted to handle person identifiable data, must be configured with an approved firewall and anti virus software. (Protection against other malicious software is also recommended).
- Laptops and removable media must not be left unattended at any time when in use.
- Laptops and removable media, when not in use, must be locked away securely.
- Any loss of laptop or removable media must be reported immediately using SS PCT approved incident reporting and management arrangements.
- All person identifiable data, where allowed on laptops and removable media, must be securely erased before being reassigned or disposed. Follow SS PCT disposal policy and procedures.

(d) Personal Digital Assistants (PDA's)

These devices are desirable and can be a prime target for theft. They are also easily misplaced or lost. Consequently, great care should be exercised with these devices.

- PDA's must not be used to store person identifiable data
- Any information that is held on the PDA should be kept to a minimum.
- The SS PCT approved procedure must be used for transferring information between the host system and the PDA.
- All PDA's must be registered and authorised by SS PCT responsible officers (Personally owned PDA's must not be used)
- All PDA's must be configured with an approved firewall and anti virus software (protection against other malicious software is also recommended)
- PDA's must be password protected using a strong password; at least 6 alpha numeric characters. Passwords must be changed regularly. Do not share passwords or security tokens.
- PDA's must not be left unattended at any time when active
- PDA's and associated removable storage media, when not in use, must be locked away securely (both on and off site)
- Any loss of a PDA or its removable storage media must be reported immediately using SS PCT approved incident reporting and management arrangements
- SS PCT transfer and disposal policy and procedures apply to PDA's.

Further information

If you require any further information on Safe Havens, or have any concerns about their use, please contact the Caldicott Guardian (Director of Quality and Performance) at South Staffordshire PCT Headquarters (01889 571700) or for provider arm the Caldicott Lead Head of Nursing & Operations. Merlin House 01827 306311

SAFE HAVENS

FAX MACHINES LOCATED IN SAFE HAVENS

- PCT HQ Quality & Performance and Public Health Directorates
- Langton / Spires DNs
- Albert Road Community Office
- Hednesford Clinic
- Burntwood HVs/DNs
- SRP Rehab
- Tamworth HC HVs
- Penkridge HC
- Sandy Lane HC
- Trentside (nursing)
- Discharge liaison SRP
- Infection control SJCH
- Medical records SRP
- Medical records SJCH
- Anglesey House Burton
- Tutbury HC
- Barton Health and Community Centre HV/DN
- BURDOC – Night Service Team
- Branston Medical Centre
- Rapid Response SRP
- Peel Practice
- Stoneydelph DNs
- Salters Meadow
- Cannock Block C
- Merlin House (risk team)
- Wilnecote HC
- SRP MIU
- Spires Practice
- Renal
- SJCH Outpatients
- Rehab SRP
- Balance St Surgery
- Bridge Surgery
- Imex ELS/Wheelchair
- Wetmore Rd Surgery
- Stapenhill Surgery
- Cross St Clinic
- Tamworth HC – Speech and Language
- Greenhill HC - Speech and Language
- Norton Canes