SAFE HAVEN PROCEDURE – CPG50(C)

Appendix 1

1.0 Safe Haven Incoming and Outgoing Faxes

Fax is only permitted for use in the Trust Pharmacy Service.

2.0 Safe Haven Electronic Information (transfer by Email)

2.1 Do's for Electronic Information

2.1.1 Confidential information can be sent between NHSmail accounts – but only when essential to service delivery. Where Line Managers / Directors expressly require information to be transferred via this method the ITT Servicedesk should be contacted, who will arrange for an NHSmail account to be set up. (The email will be encrypted automatically).

2.1.2 Confidential information transferred by email must only be carried out using specifically registered, authorised and secure devices (e.g. encrypted desktop or laptop) and only in accordance with Trust approved policies and procedures. (Personally owned devices must not be used under any circumstances).

2.1.3 Suitably approved back up and fail safe facilities must be in place and operating satisfactorily before confidential information is transferred by email.

2.1.4 Where transfer of person identifiable confidential information by email is allowed; this must be sent as encrypted / password protected attachments (and not in the body of the email) through NHSmail accounts, wherever possible.

2.1.5 Emails must be checked to ensure that responses / replies are only sent to the relevant recipients and that the content of the email does not include irrelevant email "runs" (additional information included within the email).

2.1.6 Where transfer of confidential information by email is allowed, a secure "mechanism" must be in place to trace all confidential information.

2.1.7 The address of the recipient must first be confirmed, together with a test message also confirmed.

2.1.8 When emails are used to transfer confidential information the email subject should clearly be marked "confidential".

2.1.9 The subject window of confidential information transferring by email must be identified as "***SAFE HAVEN***". Best practice requires that no identifiable information is used within the body of the email unless it is absolutely essential in which case initials can be used unless these initials can identify an individual.

2.1.10 Email transferring confidential information must carry a Trust approved disclaimer for confidential information (see below 4.2.1.1).

2.1.11 The following email domains are secure for sending person identifiable information to external organisations:

Secure email domains in ***central government***: *gsi.gov.uk, *gse.gov.uk, *gsx.gov.uk. The ***Police National Network/Criminal Justice Services*** secure email domains: *.police.uk, *.pnn.police.uk, *.scn.gov.uk, *.cjsm.net. Secure email domains in ***local government / social services***: *.gcsx.gov.uk
However these are subject to change so please check first.

2.1.12 The intended recipient must adhere to the principles of safe haven (i.e. to ensure that confidential information is only viewed by persons authorised to view such information).

2.1.13 Confidential information sent to the Trust by e-mail must be virus checked before it is opened.

2.1.14 Confidential information sent to the Trust by email must only be stored on Trust registered secure network servers. (It must not be stored on PC's, laptops, ipads and other portable devices or removable media).

2.1.15 **Disclaimer: "***This document and any attachments to it are confidential and privileged and intended solely for the use of the individual or entity to whom they are addressed. They should not be disclosed, copied or distributed without the prior authorisation of the author. Use of / action taken in relation to its contents is strictly prohibited and may be unlawful. In the event of mis-direction please notify sender."*

2.2 **Don'ts for Electronic Information**

2.2.1 Confidential information must not be sent by email unless it is encrypted / password protected to NHS approved standards and using software authorised and configured by the Trust.

2.2.2 Staff are not permitted to send confidential information in relation to patients, employees or the public via Internet Mail (e.g. Yahoo, Hotmail etc.).

2.2.3 Confidential information must not be sent in the open body of the email. An encrypted / password protected attachment must be used or sent via NHSmail.

2.2.4 Confidential information must not be sent to share or group email boxes (unless all those with access to the mail box have the necessary security authorisation and access).

2.2.5 Confidential information must not be forwarded by e-mail to any person or organisation that is not specifically authorised to review and view that information.

3.0 Safe Haven Incoming and Outgoing Post

3.1 **Do's for Incoming Post**

3.1.1 Deliver incoming post efficiently and quickly to the recipient. If the recipient is unavailable the designated deputy must take responsibility for the post.

3.1.2 If the post is marked "Private and Confidential" to a named recipient, only the named recipient should open the post (unless prior arrangements have been agreed).

3.1.3 If the named recipient is known to be absent for a period of time post should be redirected to the Team Manager.

3.1.4 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 to the recipient.

3.1.5 Once the post has been passed over, it is the owner's responsibility to ensure the safe keeping of the confidential information, using their own safe haven locked cabinet / room / drawer (see notes on storage of information).

3.1.6 A return address must be printed clearly on the internal postal envelope to ensure the post can be sent back to the original sender if received in error by the wrong recipient.

3.2 Do's for Outgoing Post

3.2.1 Make sure outgoing post is addressed to the correct recipient.

3.2.2 When sending confidential information to another organisation always mark with "Private and Confidential – To be opened by Addressee only". The recipient's name and full postal address should be clearly **printed** on the envelope or a window envelope used. This information should only be sent by 1st class post and NOT 2nd class post.

3.2.3 Include a return address to ensure that if the envelope is received in error, the recipient can return the post without opening the envelope.

3.2.4 For clinical information consider addressing to the 'Team' rather than an individual, if appropriate and depending upon the urgency of the correspondence.

3.2.5 When sending mail that is confidential but to a number of people, e.g. a team or service, the correspondence and the envelope should be clearly marked "Private and Confidential".

3.2.6 Sensitive person-identifiable information should only be sent by "Recorded / Special Delivery" service, which includes both a Track and Trace and an electronic Proof of Delivery (ePOD) facility, so that the location of the package can be determined through its journey, and the final delivery signature checked (e.g. Special Cases, Health Records, Child Health Records, etc). appropriate stationery, such as reinforced envelopes or document wallets when necessary. Check that the name and full postal address of the recipient is Printed clearly on the package or written in permanent marker using block capitals on a plastic document wallet.

3.2.7 Where there are several packages / particularly large packages the sender may need to consider the use of authorised courier services (advice on authorised courier services can be obtained from the Trusts Records Manager). It is

essential to confirm that the courier service has tracking systems in place, including recording of collection / delivery and traceability of the package.

3.2.8 When sending confidential information to another organisation you must stamp or mark the envelope:

SAFE HAVEN
Private and Confidential / Addressee Only
If undelivered, please return to sender:
(Sender's address – use the designated PO Box number for your site)

3.2.9 Post intended for patients, residents, their relatives or carers should not have any Trust identifiable return address / franking marks on the envelopes in order to maintain the confidentiality of that person (**use the designated PO Box number for your site**). It is noted that this is not always under the control of the Trust where post is handled on the Trust's behalf by other organisations.

3.2.10 Teams should undertake risk assessments on the types of correspondence they send to assess which correspondence would need to be sent "Recorded / Special Delivery". Highly sensitive information (e.g. full assessment reports / sensitive person information, e.g. health or physical condition, sexual life, ethnic origin, religious beliefs, political views or criminal convictions) may need to be Recorded / Special Delivery whereas, e.g. an appointment letter, containing minimal personal information could be sent by normal postal services.

3.2.11 When sending confidential information using the internal post, ensure that the information is placed in a sealed envelope and then placed in the transit envelop with "Private and Confidential" written on the outside.

3.2.12 Call the recipient to ensure the confidential information has arrived or ask the recipient to call when they have received the confidential information, where appropriate.

3.3 Don'ts for Outgoing Post

3.3.1 Leave confidential post unattended in an open area.

3.3.2 Send confidential information to insecure locations.

4.0 Safe Haven Verbal Communications, Phones and Answer Phones

4.1 <u>Do's</u> for verbal communication, phones and answer phones

4.4.1 Try not to disclose confidential information over the phone because of risk involved (e.g. being overheard, inadvertent disclosure of confidential information, disclosing confidential information in an inappropriate manner, etc.).

4.4.2 Try to have phones away from the reception area. If this is not practical, take reasonable steps to protect a patient's/residents/ client's or the organisation's confidentiality whilst speaking on the phone.

4.4.3 Ask questions over the phone that require the patient/resident or client to answer rather than giving them details which they need to confirm e.g. try not to say "Is that Joan Bloggs of 15 Town Road, Any Town?". Instead ask the patient/resident or client who they are and where they live and do not repeat the information out loud.

4.4.4 If you receive a call from another health professional, confirm their identity and their reason for asking before giving out any confidential information.

4.4.5 If you have any doubt as to the identity of the caller, call them back using a published telephone number (rather than one they quote).

4.4.6 Put callers on hold so they cannot hear other confidential conversations that may be going on in the office.

4.4.7 In face to face situations ask for proof of identity and once verified ensure that discussions take place in private locations and not public areas, common staff areas, lifts etc.

4.4.8 It is vital that the correct patient/resident is being discussed. The wrong information may be given out if there is a misunderstanding so make sure first.

4.4.9 If you receive a call from someone claiming to be a relative and asking information relating to the condition of the patient or resident, check with the patient person for permission (consent) to disclose. Until you have this permission (consent) you must not confirm or deny whether you have a patient or resident with that name so that you do not breach confidentiality. If this is not possible then do not disclose any information.

4.1.10 If the Police request any patient or resident identifiable information they should be directed to the Head of Records Management / Legal Manager.

4.1.11 Media requests for patient or resident identifiable information must always be referred to the Trust DPO/ Records Manager or Information Governance Manager. Staff are not authorised to release any identifiable information to the media or press.

4.1.12 Ensure before information is given out that the enquirer has a legitimate right to have access to the information.

4.1.13 Ensure answer phones are located in a secure area and are only accessible by authorised personnel.

4.1 <u>Don'ts</u> for verbal communication, phones and answer phones

4.2.1 Repeat any confidential details that a patient/resident gives you if others may hear them e.g. there is no need to mention forenames and surnames out loud in the same conversation.

4.2.2 Have the phone switched on to "speaker" mode, turning a confidential call into a "tannoy" message.

4.2.3 Assume permission (consent) if you are asked to give patient /resident information to a relative – check with the patient/resident or your manager first.

4.2.4 Leave messages containing confidential information on answering machines unless permission (consent) has been given to do so.

4.2.5 Leave messages containing confidential / sensitive information on white boards / notice boards.

4.2.6 Do not store staff personal numbers on the phone particularly if it is in a shared area or office.

5.0 Safe Haven Information Storage

5.1 **<u>Do's</u> for information storage**

5.1.1 Ensure all confidential information is stored in locked cabinets / rooms / drawers. There are designed safe havens for confidential information. A clear desk procedure should, where possible, be in place.

5.1.2 All sensitive records must be stored face down in public areas and not left unsupervised at any time.

5.1.3 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 cabinet / room / drawer (or their own) as quickly as possible.

5.1.4 Keep a note if any information is transferred so that it can be tracked if necessary.

5.1.5 Continually assess whether information needs person identifiers or whether it can be anonymised.

5.1.6 Nominate a person to be responsible for holding the keys to the locked cabinets / rooms / drawers. This person will be responsible for the safe-keeping of the information within the cabinets / rooms / drawers.

5.1.7 Audio tapes or CD's awaiting text should be kept in a locked cabinet / room / drawer and erased immediately after use.

5.1.8 Protect confidential information by encryption (or other Trust approved protection methods) and strong authentication.

5.1.9 Only transfer confidential information in accordance with Trust approved policies and procedures.

5.1.10 Store confidential information on the Trust network servers, in restricted access folders (refer Information Governance and Security Procedure and Procedures)

5.1.11 Only use authorised and encrypted laptops / ipads to process confidential information. The level of protection that the encryption provides must meet the

minimum as laid down by the Department of Health and Connecting for Health guidelines in relation to the electronic transfer of person identifiable information / confidential information.

5.1.12 The laptops / ipads should also be configured with anti virus / anti-malware software, which is active.

5.2 **Don'ts for information storage**

5.2.1 Copy to or hold information on removable media (e.g. USB devices, laptops, ipads, portable hard drives, Blackberry mobile phones etc.), unless it is absolutely necessary or has been authorised. Only use encrypted removable media issued / approved by the Information Governance Team or ITT Team. Personally owned removable media must not be used in any circumstances.

5.2.2 Leave any approved removable media (e.g. USB devices, laptops, ipads, dictaphones or portable hand held drives etc.) containing sensitive / person-identifiable information accessible or in view.

5.2.3 Label the approved removable media (e.g. USB devices, laptops, ipads, portable hard drives etc.) in any way which might identify that the device holds confidential information.

5.2.4 Upload any incoming removable media (e.g. USB devices, laptops, ipads, portable hard drives etc.) from other organisations until the security has been checked by the anti-virus.

5.2.5 Hold any confidential information on local drives (C:// Desktop or My Documents, My Pictures, My Videos, etc.). (Only store this information on Trust network server(s), in restricted access folders).

5.2.6 Leave confidential information unattended at any time.

5.2.7 Leave documents unattended at the photocopier if person identifiable information is present.

5.2.8 Leave confidential information in any area where it may be seen or looked at by unauthorised persons, even for short periods.

5.2.9 Leave files open when not in use.

6.0 Safe Haven Shredding

6.1 **Do's for shredding**

6.1.1 Destroy confidential information in a correct way. Use a **cross-cutting** shredder for the destruction of confidential information.

6.1.2 Make sure everyone knows how to use the cross-cutting shredder and what type of information should be destroyed using it.

6.1.3 Make sure that records are kept for the specified length of time. (Department of Health: NHS Records management – Code of Practice Parts 1 & 2) and then shredded.

6.1.4 Treat surplus or spoiled photocopies of confidential information as confidential waste.

END