NHS
Cambridgeshire Community Services
NHS Trust

Information Sharing Guide

Handling Confidential and Sensitive Information

Cambridgeshire Community Services NHS Trust: providing services across Bedfordshire, Cambridgeshire, Luton, Norfolk, Peterborough and Suffolk

Handling Sensitive and Confidential Information.

The Trust has standards about how personal confidential information is transferred whether this is via post, fax, email, removable device (eg USB stick or CD), text message or on laptops to ensure such transfers are secure and will protect the confidentiality of our service users and/or staff.

The Trust's policies and procedures contain full and detailed guidance and these are available on the Trust's website.

This guide sets out the steps you should take when sending or receiving information via any of the above routes.

Reporting Information Governance/ Confidentiality Incidents.

Any person who experiences, discovers, witnesses or is notified of an incident/ near miss should inform the person in charge. **The person in charge is responsible for ensuring the incident is recorded using the Trust's Datix reporting system.**

https://nww.riskreporting.ccs.nhs.uk/index.php?module=

By Post

1. Internal Mail: use a robust envelope (not an Internal Mail envelope), double-envelope where size or weight dictates; mark "Private & Confidential", clearly print name and full address of recipient (and sender on reverse) and request acknowledgement of safe receipt.

2. External Mail: as above, use a new robust envelope and send by either "Recorded Signed For" or "Special Delivery" or private courier. Due to the cost difference, the best option should be selected following a local risk assessment. Safe receipt should always be confirmed. Routine clinical correspondence may continue to be sent by first or second class post.

3. Removable devices and DVD's sent by post: must be encrypted and sent by 'tracked post' or courier.

4. Opening incoming post: Where confidential mail is received (eg marked Personal, Private & Confidential; In Confidence, etc) this should only be opened by the addressee unless authority has been delegated. Local arrangements must be made to deal with post received in the absence of addressees.

By Fax

1. Safe Haven Faxes: are those which are sited where the general public do not have physical access; and/or which are switched off at night; and/or are in a locked room/location thus preserving the confidentiality of incoming documents.

2. Unattended Fax Machines: Always ring before transmitting a fax containing personal confidential information to ensure the machine will be attended until receipt. Always use a cover sheet. Always request the recipient to phone to acknowledge safe receipt. If appropriate, request a report sheet to confirm that the transmission was sent.

3. Frequently used numbers: should be identified and programmed into the fax machine's 'memory dial' facility to reduce risk of misdialing/ misdirection.

4. Incoming faxes should be removed from the machine immediately upon receipt and passed to the addressee without delay.

By email

1. NHSmail: It is Trust policy to use NHSmail when emailing PID and both sender and receiver have to have NHSmail accounts. Trust Policy recommends using an NHSmail generic account as this minimises risk of misdirection and allows for emails to be accessed by more than one authorised person (useful when staff are out of office or have unplanned absences).

The sender must always confirm the NHSmail address of the recipient (i.e. DO NOT assume it is firstname. lastname@nhs.net; always use the directory on the NHSmail website to check). To arrange for a personal or generic NHSmail account to be set up, please contact the IT service desk.

2. The receipt facility should be used for transfers of personal confidential information.

3. It is acceptable to use some non-NHSmail accounts which are similarly secure for transfer of personal confidential information. An example of this is " ..... gsi.gov.uk". Please check the Information Security Policy on the website for up to date versions and list.

4. If sending personal confidential information via email to any other account where there is no NHSmail account or other secure network, always use a Trust approved encryption method, which will detail the encryption to be used and how to communicate the password or passphrase. Please contact your local IT service desk for guidance with this.

5. Whatever route the email takes, the subject line of the email must never contain personal confidential information.

6. If you receive an incorrectly addressed email via NHSmail, you must inform the sender so that they can correct their records, you must then delete the email from your inbox.

By telephone

1) Confirm the name, job title, department and organisation of the person requesting the information and also the reason for the information request, if appropriate.

2) Never give any personal confidential information over the phone unless you are completely satisfied of the identity of the caller and their entitlement to the information. If you are in any doubt consult your manager. Unless the caller is well known to you, his/her identity should always be established by ringing the person back (via a manned switchboard - not dialing the number they have provided and never to a mobile).

3) Check whether the information can be provided. If in doubt, tell the enquirer you will call them back. Provide the information only to the person who has requested it (do not leave messages unless advised that it is appropriate to do so). Only disclose what is absolutely necessary.

4) Ensure you record your name, date and time of disclosure, the reason for it and who authorised it. Also record the recipient's name, job title, organisation and telephone number.

5) Recorded telephone messages containing confidential personal information (eg names and addresses of applicants phoning for a job or patient/service user details) must be properly secured so that only those entitled to listen to the message may do so.

6) Any message books used to note messages for absent staff should always be stored securely. Any clinical information must be recorded in the patient/service user's Health Record:

a) Always ensure the patient/service user is aware of the risks associated with communicating in this way and that this has been agreed and documented as part of the patient/service user's Health Record.

b) Standard mobile phone exchanges: a written record of the content of the text message, sent and received, should be made in the patient/service user's Health Record.

Leaving messages on patient answerphones

The Trust recognises the fact that staff may need to leave messages on both home and mobile telephone answerphones in order to communicate with patients. However, the Trust must comply with Data Protection legislation in order to protect patients, staff and the Trust.

If you are contacting a patient for the first time and they are not expecting a call from your service then:-

- It is only acceptable to leave your full name; first name followed by family name and contact number.
- You must not leave your designation* details as this could identify the type of care the patient is due to receive.
- Another person may pick up the message and not realise the patient was undergoing treatment. The patient may then be entitled to go to the Information Commissioner and state that the Trust was in breach of their Data Protection rights.

If you are contacting a patient for the first time and they are expecting a call from your service then

- On first contact leave your full name first name followed by family name and telephone number.
- If you receive no response leave a further message with your designation.
- As the patient was expecting you to make contact, it could be deemed that they have given implied consent.
- As the professional you need to make this judgement based on the patient's needs.
- Once you have spoken with the patient, then you can ask permission to leave messages on their answerphone. If you have consent from the patient either verbal or written then it is acceptable to leave your name first name followed by family name, designation, and contact number as well as any agreed information on a patient's answerphone.

For mobile phones the Trust would not recommend you leave any clinical or personal identifiable information as messages. Handsets can change frequently, be loaned out or passed on by the patient.

Other means

By portable IT equipment

By Removable Devices e.g. USB data sticks, COs, DVDs Only Trust approved encrypted USB data sticks should be used. USB sticks must be a last resort for the short term transfer of data. They must never be used for long term storage. COs, and external/removable hard drives containing personal information must be encrypted using a Trust approved encryption method. If any removable device containing personal data has to be sent by post it must be encrypted and sent by 'Special Delivery' or private courier only. NHS guidance does not allow for 'Recorded Signed for Delivery'.

By Portable Equipment (Laptops, Blackberries) These must be encrypted and be treated with extreme care and vigilance to avoid the risk of loss. Laptops must not be left in a vehicle unattended and should be transported in the vehicle boot, out of sight. Portable equipment must never be left in a vehicle overnight. In the event of loss, this must be reported to your line manager and IT service desk immediately.

Person to person

1. Personal confidential information should only be taken off site when absolutely necessary, or in accordance with local policy.

2. Where appropriate, record what information you are taking off site and why, and if applicable, where and to whom you are taking it.

3. Information must be transported in an appropriate robust bag, case or container.

4. Never leave personal confidential information unattended or on view in vehicles.

5. Ensure the information is returned to the originating site as soon as possible and record that it has been returned, where appropriate.

For further information about this service contact:

Information Governance Team
Cambridgeshire Community Services NHS Trust
Unit 3, Meadow Park
Meadow Lane
St Ives, Cambridgeshire PE27 4LG

Contact: 01480 308203
Email: CCS-TR.accesstorecords@nhs.net

You must read and comply with the Guidance on using Mobile Communication Devices DN186 which is available on the Intranet. Every member of staff has an obligation to protect confidentiality.

If you require this information in a different format such as in large print or on audio tape, or in a different language please contact the service on the details above.

If you have any compliments about this service or suggestions for improvements, contact our Patient Advice and Liaison Service on 0300 131 1000 (charges may apply depending on your network) or email: ccs-tr.pals@nhs.net.

For free, confidential health advice and information 24 hours a day, 365 days a year please contact NHS 111.

Website: www.cambscommunityservices.nhs.uk

Code No: 0440 - May 2018 (v1.3)
Date of Production: December 2016
Date of Review: December 2019