Transfer of Confidential Information

1. Every care should be taken when transferring confidential, personal identifiable information both internally and externally
2. Ensure that all envelopes are sealed, addressed correctly (addresses should include a named person, a title, department and location) and be clearly marked 'confidential'. Consider the documentation being transferred, for example, do you need to use secure tamper proof packaging for bulky documentation eg copies of health records
3. When re-using transit or previously used envelopes, ensure that any "old" addresses are deleted to assist the documents reach their correct destination. Think about the sensitivity of the documents and whether it would be more appropriate to use a new unused envelope that can be sealed and addressed accordingly.

Email (see also Top Tips for Email)

1. Ensure that when selecting recipients from the "email address book" you have chosen the correct intended recipient
2. Whilst Outlook may appear to offer a "recall" facility this function does not prevent an incorrect recipient from reading the message and/or attachments.
3. Staff must only transfer person identifiable information outside the trust electronically if the method of transfer is encrypted (encrypted email or other encryption methods – see IM&T policy)
4. Encryption passwords must always be sent separately
5. Contact the IT service desk for more information.

Social Media

1. Reflect our values of rights, respect and responsibilities; respect yourself, the people you work with, our service users, their carers and families. Maintain patient and colleague confidentiality
2. Be safe – don't publicise your own or anyone else's personal details, such as home address, date of birth etc
3. Do not post photos/videos of service users, carers or staff without consent
4. Do not reference another colleague or their work without their approval

If you are publishing opinions relating to work or the trust explain the context of why you are doing so, e.g. in your professional capacity or experience

5. Do not use language or post comments that are offensive, inflammatory or provocative; remember that even humorous comments can be misinterpreted

Do not break the law (this includes libel, appearing to approve of illegal activity and contempt of court).

6. Do not make any commercial endorsement or promotion of any product or service that could compromise the trust
7. Always remember that it's not only your reputation at stake, but also the reputation of the trust.

T.H.E. I.G. C.O.D.E

Think – when using personal information

Handle – information securely

Encrypt – all laptops and memory sticks

Information – if it's personal, it's private

Governance – you are accountable for personal information

Confidential – prevent unauthorised disclosure

Overheard – remember, sound travels

Do not share passwords or smartcard PIN numbers

Everyone has a responsibility

To find out more on how to handle personal information and where to get further help, please visit www.merseycare.nhs.uk

Mersey Care NHS
NHS Foundation Trust

T.H.E. I.G. C.O.D.E.

TOP TIPS FOR INFORMATION

KEEPING IT CONFIDENTIAL

If it's personal, it's private

www.merseycare.nhs.uk

Telephone

When telephone enquiries are received asking for disclosure of personal information, the caller should be asked to put their request in writing, where applicable. Where requests have to be dealt with more quickly, you must follow these rules:

1. You are certain you can legally disclose the information and that the person who is requesting that information has a legal right to receive it
2. You are certain the caller is who they say they are, you can do so by carrying out checks

a) If the caller is a patient or an individual for whom the department holds personal information, you must verify personal details that only the caller would know

b) If the caller is part of another organisation, obtain their name and the main switchboard number of that organisation (via the phone book or other media) and then ring back

3. In all cases you must only provide the minimum amount of information necessary
4. Ensure all conversations remain private:

a) Exercise caution and discretion when using the phone
b) Ensure sensitive conversations are not overheard, even by colleagues
c) Only mention the patient by name if essential

5. If the caller is very persuasive and authoritative:

a) Ask yourself do you have the authority to deal with this? Don't be pressurised into giving out information. Say you will ring them back and then check with your line manager.

b) If in doubt, ask your line manager, not your colleagues.

c) If challenged by the enquirer for not giving information, remain calm and polite. Clearly state that you do not have the authority to disclose the information.

Answer Phones

You must only leave a message on a service user's or individual's answer phone if it is urgent. If this is the case, leave your name and number only – do not say that you are from Mersey Care NHS Trust.

If an internal answer phone is used, make sure the caller's message is not broadcast across the office. Similarly voice mail should be code protected and only accessed by authorised staff. Treat the access code like a computer password – securely.

Faxes

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

1. Telephone the recipient of the fax to confirm the number you have is correct.
2. Request a colleague to check the number you enter is correct
3. Ensure the fax header states who the information is for and mark it 'private and confidential'
4. Send the fax transmission
5. Ring the fax recipient to confirm receipt.

Post

Take care when posting patient identifiable information. This includes internal post, Royal Mail or external carriers. Consider the sensitivity of the information and whether it needs to be sent recorded or special delivery.

1. Remember to mark all post as 'confidential' if it contains personal information
2. Seal the envelope. Do this even for internal post
3. Address the envelope fully and accurately
4. If a window envelope is used, make sure only the address is seen. No other information should be visible
5. Do not dispose of any patient identifiable information in general waste bins. Dispose of it carefully, for instance in confidential waste bags or shredding.

Talking to Others

Working in public areas:

1. Never identify a patient by name within listening distance of other people who are not involved in the conversation.
2. If discussing service users between colleagues, only identify the patient by name if essential.
3. When talking to a patient, be sure to respect their privacy. Suggest talking in a private room or area if this seems appropriate.
4. Never divulge private information without permission, even to a member of the service user's family. For instance, if someone asks "has my wife attended an appointment with Dr Smith today" – the response should be similar to "I am sorry, but we can't discuss personal information with anyone but the patient". (The exception is of course, if you have permission from the patient to share the information).

Computers/Mobile Devices

Access to any computer must be password protected and passwords must not be shared.
Computer screens must not be left in view so members of the general public, or staff who do not have a justified need to view the information, can see personal data.

1. Computers or laptops not in use should be switched off or should be locked down (by pressing ctrl, alt and delete simultaneously on your key pad)
2. Laptops, iPads and mobile devices should be kept secure in locked rooms or cabinets or in a safe environment (where members of staff are present at all times)
3. Information held on any laptop, iPad or mobile device must be password protected These should not be left unattended at any time where they can be open to theft
4. Computers and mobile devices must not be sent outside the trust for repair
5. Old computers and mobile devices must have any confidential information permanently deleted so that the information cannot be recovered
6. Only trust owned devices may be connected to the network
7. Audit trail functionality on trust systems is in operation to identify and detect any unauthorised access to records.

CDs and Memory Sticks

1. All staff must only use these devices in accordance with the IM&T Security policy ie trust owned
2. Secure encrypted memory sticks are available by contacting IT service desk
3. These should only be used in computers protected with port control and anti-virus software
4. All portable devices should be locked away when not in use
5. If a device no longer works, do not throw it away. It must be disposed of correctly by contacting the IT service desk to arrange secure disposal
6. Do not use the device as a primary means of storage.