Keeping Confidential Information Secure

Good Practice

Confidential information must:

- **Not** be shared or discussed with, or in the presence of, anyone who does not need to know, or is not specifically authorised to know that information.
- Have appropriate control applied, having regard to professional ethics and patient consent. Applying formal access controls for clinical records and statutory requirements.
- Have appropriate control applied over the disclosure on non-patient information e.g. staff, relative, visitors in accordance with statutory requirements.
- **Not** be shared with parties outside the NHS e.g. solicitors, insurance companies, employers, police without the written consent of the individual concerned unless there are specific powers to do so.
- Always be stored in a secure location, preferably a room that is locked and in some cases alarmed when unattended.
- Not to be taken home or removed from the Trust without specific authorisation, this specifically applies to patient's health records or patient data.

For all types of records, staff working in areas where personal records may be seen must:

- Shut/lock doors and cabinets as required.
- Adopt a "clear desk" policy where possible.
- Wear Trust identification badges or other authorised identification
- Query the status of strangers.
- Know who to tell if anything suspicious or worrying is noted.
- **Not** tell unauthorised personnel how the security systems operate.
- **Not** breach security themselves.

Manual records must be:

- Formally booked out from their normal filing system.
- Tracked if transferred, with a note made or sent to the filing location of the

transfer.

- Returned to the filing location as soon as possible after use.
- Stored securely within the clinic or office, arranged so that the record can be found easily if needed urgently.
- Stored securely when not in use so that contents are not seen accidentally.
- Inaccessible to members of the public and not left even for short periods where they might be looked at by unauthorised persons.
- Held in secure storage – with permitted access. The availability of a secure means of destruction, e.g. shredding, are essential.

With electronic records, staff must:

- Always log-out of any computer system or application when work on it is finished.
- **Not** leave a terminal unattended and logged-in.
- **Not** share logins with other people. If other staff have a need to access records, then appropriate access should be organised for them – this must not be by using others' access identities.
- **Not** reveal passwords to others.
- Change passwords at regular intervals to prevent anyone else using them.
- Avoid using short passwords (use 6-8 characters), or using names or words that are known to be personally associated with them (e.g. children's or pet names or birthdays).
- Always clear the screen of a previous patient's information before seeing another.
- Use a password-protected screen-saver where possible to prevent casual viewing of patient information by others.
- Protect information from the view of others as far as possible, particular care when there is a visitor present.
- Ensure that unwanted confidential printouts are shredded using a cross cutting shredder where possible and disposed of in confidential waste bins and in accordance with Trust policy on record disposal.
- Ensure that electronic media such as CD and Computer hard drives are disposed of in accordance with IT policy and procedures.

Telephone enquiries should be validated by:

- Checking the identity of the caller.
- Checking whether they are entitled to the information they request.
- Taking the calling number, verifying it independently and calling back if necessary.

Staff should ensure that general conversation involving discussions about individuals (including telephone) is:

- Where appropriate, undertaken in an area out of earshot of others, preferably in a

closed office.
- **Not** undertaken with anyone who is not authorised to receive the information, including family and friends.
- Restricted to the use of personal identifiers (e.g. hospital number) when in public/reception areas

Confidential information sent via internal post or in internal transit should always be:

- Appropriately addressed to a named recipient, post holder, consultant or legitimate Safe Haven (Trust nominated secure area).
- Sealed in an appropriately secure envelope/package based on sensitivity and volume
- Marked accordingly, with "Confidential" or "Addressee Only" as appropriate.
- Traced in or out and signed for as appropriate.

Confidential information sent via external post or in external transit should always:

- Be addressed fully and marked accordingly, with "Confidential" or "Addressee Only" as appropriate.
- Be sealed in an appropriately secure envelope/package based on sensitivity and volume and using tamper proof seals where practicable and appropriate.
- Be sent via an approved carrier such as NHS courier, Internal transport or recorded delivery for any confidential information sent in quantity such as patient health records or a collection of patient information on paper or printout, , CD or other media. Obtaining a receipt as proof of sending/delivery is advised where possible.
- Traced in or out and signed for as appropriate.
- Have appropriate authorisation for leaving the Trust particularly in the case of patient's health records.

Staff wishing to send or receive confidential patient information via fax must:

- Adhere to the Trust Safe Haven Procedures.
- Only send personal identifiable data to a recognised NHS Safe Haven (nominate secure area) fax number.
- Remove all identifiable data if not sending to a recognised NHS Safe Haven number
- Address the fax to a named recipient.
- Always check the number to avoid misdialling, check the number is correct and current if stored in a fax memory prior to sending.
- Ensure that trust fax machines are placed in secure locations, preferably within the boundary of a Safe Havens (Trust nominated secure area). As a minimum fax machines should be locked when unattended, switched off outside normal working hours or safely secured in lock cupboards if left switched on.

Staff using E-Mail must: (refer: Internet/Email Access and Use Procedural Guidelines (CPG50(B))

- Not e-mail person identifiable information externally to the Trust unless standard encryption software has been implemented and approved by the IT department. NHS mail is the approved method for transferring person identifiable information; otherwise, password protection and encryption are advised. Only e-mail person identifiable information when the Caldicott Principles are applied (anonymised where possible) and by placing the identifiable information in a password protected attachment and not including person identifiable information in the subject line or body of the email.
- Check to ensure that the recipient is authorised to receive the data (be careful of shared mailboxes).
- Ensure that extra care is taken to ensure that it is sent to the correct person (use of personal address books is recommended).

Staff working offsite:
(In relation to confidential data (inc. patient, staff, corporate, full or part records)

- Staff who have a need to carry paper records offsite should work in line with the Trusts' Transportation (CPG9f) and Data Protection (CPG59) Procedures.
- Should only carry paper data if electronic alternatives are unavailable
- Should seek advice from Line Managers / Information Governance Team if in doubt.
- All Items should be transported in locked boot of car and removed and taken with the staff member on arrival.