TFR Pharma

PembrokeCastle PHARMACY MENDUSPHARMACY

Data Handling, Record Keeping & Disposal Procedures v.2.0

Statement Prepared by:	Statement Approved by:	Date Next Review Due:	1/3/26
Mark Roberts	Nathan Raymond		
Date Version Prepared:	Date Version Approved:	Date Review Takes Place:	
19/2/24	26/6/24		

Scope & Purpose

This document outlines data handling procedures. These procedures are in place to help prevent unauthorised access to information, loss of information, unauthorised disclosure of information or breach of legislation. These procedures apply to all staff working across the Pharmacy group, not just those staff working in a Pharmacy.

1. Maintaining confidentiality of data received (safe havens)

The term safe haven is a term used to explain either a secure physical location or the agreed set of administrative arrangements that are in place within the pharmacy group to ensure confidential personal information is communicated safely and securely.

The dispensary is the pharmacy's 'safe-haven' and is the location for patient information to be securely received, for example faxes containing patient sensitive information should be sent to the dispensary fax machine – typically used as a last resort, given there are other technology alternatives which may be available such as encrypted email if appropriate processes have been arranged as required. All Post, Communications & Health Board/GP/Medical Practice communications should be opened in the dispensary and out of sight of main public access areas of the pharmacy shop.

A. When paper-based information is received it should be stored securely, as soon as practical, for example:

(i) Information moved from the front counter to the secure dispensary area.

(ii) Manual patient records such as MUR forms should be locked in an appropriate file storage when not in use.

B. Computers should not be left on view or accessible to unauthorised staff:

(i) Be careful where you site your computer screen: ensure any confidential information cannot be accidentally or deliberately seen by visitors or staff who do not have authorised access. Be especially careful with computer screens in the consultation area. It is advisable to use a screen diffuser to obscure patient view of computer screen.

(ii) Always keep your password confidential and do not write it down. Do not share passwords.

(iii) Password protected screensavers should be used where possible.

(iv) Laptop computers should be locked up when not in use. Wherever possible a physical laptop security cable should be attached to prevent physical theft of device.

C. Ensure that all waste containing patient-identifiable information, for example the right-hand side of prescription forms and duplicate labels is securely disposed in the approved secure waste disposal consoles/bags to await secure disposal. Waste medicines received from patients or waste bottles where administration was supervised in the pharmacies should be placed in the controlled waste (DOOP) bin. There is no need to remove patient-identifiable information such as labels before placing the waste is placed in the in the controlled waste (DOOP) bin.

D. Ensure that confidential conversations are held where they cannot be overheard by members of the public. Ensure that sensitive medical issues are only discussed in the consultation area.

2. Only transferring data where appropriate

A. The personal information contained in transfers should be limited to those details necessary in order for the recipient to carry out their role.

B. Before transferring data, consider whether there are any patient consent requirements that must be met before the transfer is made, or not:

i. A record of consent should be maintained where required, either on the relevant form where available (e.g. the pharmacy service form, enhanced services forms etc.) or a record made on the Patient Medical Record (PMR) system.

ii. For certain scenarios, a patient may have the right to choose whether or not to agree to the use or disclosure of their personal information and the patient has the right to change their decision about a disclosure before it is made. If the patient indicates refusal to consent, they should be referred to the pharmacist who can discuss the risks if consent is withheld and consider whether there is a legal requirement for sharing or, if there is no legal requirement, whether it is in the public interest or the vital interests of the patient (or anyone else affected) to disclose information.

iii. Only staff authorised by the pharmacy as contractor should have responsibility for obtaining consent for non-healthcare purposes, for example research.

iv. If the patient has detailed questions about consent, they should be referred to the pharmacist.

v. If circumstances change, relevant to the sharing of consent, for example if there is a change of recipient, consent should be reaffirmed.

3. Securely transferring data

Consideration needs to be given to the mode of transfer and whether any specific controls are required to maintain the confidentiality of the data e.g. encryption on electronic transfers.

A. Verbal communication

i. Be careful about leaving confidential messages on answer-phones (e.g. information about the patient's medicines). It might not be heard only by the intended recipient.
ii. Be careful when taking messages off answer-phones. Ensure that the messages cannot be overheard inappropriately when being played back.
iii. When receiving calls requesting personal information: a) verify the identity of the caller, for example, where this is not a known contact, this can be done by taking the relevant phone number, double checking that it is the correct number for that individual / organisation and then calling the recipient back b) ask for the reason for the request, c) if in doubt about whether the information can be disclosed, tell the caller you will call them back, and then consult with your manager.
iv. Where information is transferred by phone, or face to face, care should be taken to ensure that personal details are not overheard by other people, including staff who do not have a "need to know". Where possible, such discussions should take place in private locations and not in public areas, for example staff room.
v. Messages containing confidential / sensitive information should not be left on notice boards that could be accessed by non-authorised staff.

B. Post

i. Ensure envelopes are marked "Private & Confidential"
ii. Double check the full postal address of the recipient.
iii. Carefully consider the method for sending confidential information based on risk of loss. For example bulk transfers of prescriptions to NHS Prescription Services must always be sent in a secure manner that enables tracking and tracing of the delivery.
iv. When necessary, ask the recipient to confirm receipt.

C. Faxing

i. Faxing may increasingly be used as a last resort as other alternatives can be more suitable**. It is now NHS practice to shift away from using faxes to a secure mail system.**
ii. If faxing personal or confidential information: a) double check the fax number, b) ensure that you mark the fax header "Private & Confidential". Always identify a named person, not a team, who needs to receive the fax.
iii. If faxing personal information to an organisation that doesn't have a 'safe haven' fax machine where information can be received securely, take extra precautions for example, let the recipient know when the fax will be sent, ask them to wait by the fax machine and confirm

receipt. Most faxes will allow 'report' sheets to be generated which also confirm the transmission was okay.

iv. If a particular fax number is going to be used regularly, store the number in the fax machines memory where possible to reduce the risk of typing errors.

v. Consider avoiding sending certain faxes to an organisation outside of their working hours where there may be no-one present to receive.

D. Communication by email

i. Transfer of personal information by email should be avoided other than where both sender and recipient are using an NHS mail account (nhs.net to nhs.net accounts) or the information is sent as an encrypted attachment.

ii. If patient identifiable information must be sent other than via NHS mail, it MUST be encrypted to NHS standards.

iii. The email header should make it clear that the information contains confidential information.

Other forms of information exchange (e.g. text messages, e-mail, IP phones etc) can be used in general operation of the business, but must not be used to send Personal Identifiable Information (PII)

4. Record keeping and retention schedules

In some cases, clinical digital data that helps care of the patient may be kept for at minimum the lifetime of the patient. NHS set out some recommended **minimum** retention periods within their **Records Management Code of Practice for Health and Social Care**. The Specialist Pharmacy Service (SPS, **sps.nhs.uk**) also have provided a detailed example record keeping document for pharmacy teams.

Staff within our pharmacy will keep records necessary in alignment with those documents unless specified otherwise within other policies.

5. Disposal and destruction

If there is no longer a valid reason to keep personal data (and the data is outside of the minimum retention period you have set) there are methods for destruction we can use. There are three common types of items that may require destruction by either us or our third-party disposal contractor. The three types are:

- paperwork;
- digital data; and
- electronic hardware (e.g. a computer hard drive).

A. Types of items to destroy

Paperwork: At the end of their lifespan, confidential paper records will be shredded and disposed of securely. The Pharmacy will either destroy itself using the shredder located in a safe haven area or use an accredited secure waste disposal contractor.

Digital data: It is just as important to get rid of electronic records as it is paper records. Make sure that you do not miss these when doing your records audits. The pharmacy computer software ensure secure deletion of digital data. Regular system maintenance checks are made to ensure system health & integrity is maintained (data disk clean-ups, de-fragmentation etc).

Electronic Hardware: Removal of confidential information from a computer or other electronic storage device is not as easy as throwing it away.

The Pharmacies Lead for IG & Data Security must ensure that all removable hardware (disk, tapes, memory sticks etc) are secured erased / destroyed before disposal.

The Pharmacies IT contractor will ensure that all memory from hard drives servers and hardware (PCs & Laptops) have been securely erased before disposal. It is recommended that hardware is disposed of through an accredited disposal company.

The removal of computer media by external companies is not permitted without contractual agreement. Hardware awaiting removal must be securely stored at the Pharmacy Admin Office and not left in pharmacy shops areas.

A certification of destruction for any computer equipment/media by the approved contractors must be obtained and filed at the Administration Office.

B. Procedures for destruction (including contracts with disposal companies)

We can perform destruction in-house and/or we use sufficiently reputable contractors. When we hire a contractor to perform destruction, we will have a terms of service with this organisation and they must provide us with certificates of destruction for the information they have taken away.

6. Data protection by design and default

The pharmacies IG Lead is responsible for setting out procedures for new processes or services in a way so that data protection is 'baked in' from the start. This may arise from any DPIAs.

Data protection by design is about considering data protection and privacy issues upfront in everything pharmacy staff do in line with **ICO guidance**.

Our DPO can advise and be consulted on any of these matters.