

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| < Insert name of pharmacy>  **Data handling, record keeping and disposal procedures** | | | | <Insert pharmacy logo> |
| Doc prepared by: | Doc approved by: | Date next review due: |  |  |
| Date prepared: | Date approved: | Date review takes place: |  |  |

|  |
| --- |
| ***About the use of this document and related resources****: This* [*data security*](http://psnc.org.uk/ds) *document assists the pharmacy’s aligment with the*[*Data Security and Protection Toolkit (DSPTK)*](http://psnc.org.uk/dsptk)*. Related pharmacy policies are at PSNC’s* [*data security templates webpage*](http://psnc.org.uk/dstemplates)*.* |

*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 in the pharmacy, not just those staff working in the Dispensary.*

**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 to ensure confidential personal information is communicated safely and securely.

The dispensary is this 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 as a last resort given there are fax alternatives which may be available if appropriate processes have been arranged as required. All post for the pharmacy should be opened in the dispensary.

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 the filing cabinet 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.

(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.

C. Ensure that all waste containing patient-identifiable information, for example the right-hand side of prescription forms and duplicate labels is cross shredded before disposal. Waste medicines received from patients or waste bottles where administration was supervised in the pharmacy 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:

1. 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.
2. 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.
3. Only staff authorised by the contractor should have responsibility for obtaining consent for non-healthcare purposes, for example research.
4. If the patient has detailed questions about consent, they should be referred to the pharmacist.
5. 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**

1. 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.
2. Be careful when taking messages off answer-phones. Ensure that the messages cannot be overheard inappropriately when being played back.
3. 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.
4. 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.
5. Messages containing confidential / sensitive information should not be left on notice boards that could be accessed by non-authorised staff.

**B. Post**

1. Ensure envelopes are marked “Private & Confidential”
2. Double check the full postal address of the recipient.
3. 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.
4. When necessary, ask the recipient to confirm receipt.

**C. Faxing**

1. Faxing may increasingly be used as a last resort as other alternatives can be more suitable (see [psnc.org.uk/fax](https://psnc.org.uk/fax)). NHS objectives include the removal of fax machines and the use of alternative methods such as NHSmail.
2. 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.
3. 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.
4. 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.
5. 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**

1. Transfer of personal information by email should be avoided other than where both sender and recipient are using an NHSmail account (nhs.net to nhs.net accounts) or the information is sent as an encrypted attachment.
2. If patient identifiable information must be sent other than via NHSmail, it MUST be encrypted to NHS standards.
3. 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)

[Specialist guidance should be inserted for other forms of data transfer in use in the pharmacy]

**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. NHSX set out some recommended **minimum** retention periods within their [Records Management Code of Practice for Health and Social Care](https://www.nhsx.nhs.uk/information-governance/guidance/records-management-code/). The Specialist Pharmacy Service (SPS, [sps.nhs.uk](https://www.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.

**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.

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

We recommend using a contractor or your IT supplier to dispose of this equipment for you. As above, ensure that you have a written contract in place and that you receive a certificate of destruction.

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

<We can perform instruction in-house and/or we use sufficiently reputable contractors. When we hire a contractor to perform destruction, we will have a written contract with this organisation and they must provide us with certificates of destruction for the information they have taken away. They will also sign a contract to say we may inspect their facility should we wish to do so.>

**6. Data protection by design and default**

The pharmacy IG lead(s) or equivalent should be involved with setting out procedures for new processes or services in a way so that data protection is ‘baked in’ from the start.

Data protection by design is about considering data protection and privacy issues upfront in everything you do in line with [ICO guidance](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-by-design-and-default/).

|  |
| --- |
| *This data security document assists the pharmacy’s aligment with the Data Security and Protection Toolkit (DSPTK). Related pharmacy policies and more can be found at:*   * [*psnc.org.uk/ds*](http://psnc.org.uk/ds)*;* * [*psnc.org.uk/dsptk*](http://psnc.org.uk/dsptk)*; and* * [*psnc.org.uk/dstemplates*](https://psnc.org.uk/dstemplates)*.*   *Pharmacy contractors with queries about the original template or questions about DSPTK may contact* [*it@psnc.org.uk*](mailto:it@psnc.org.uk)*.*  *This document is based on a template updated during: Feb 2021* |