

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| < Insert name of pharmacy>  **Code of conduct for employees in respect of confidentiality** | | | | <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)*.* |

*Please note that this document should normally be read and understood prior to the contract of employment or other confidentiality agreement being signed. If there is anything that is not clear please contact your manager.*

**Purposes of this code**

This code sets out the standards expected of staff in maintaining the confidentiality of patient information.

**Legal framework governing confidentiality and staff responsibility**

All staff have a personal duty of confidence to patients and to his/her employer.

The duty of confidence is conferred by common law, statute, for example data protection laws, contract of employment, and where applicable, professional registration.

**What is considered confidential information?**

Personal information is data from which a living individual could be identified; this may include information such as name, age, address, and personal circumstances, as well as sensitive personal information regarding race, health, sexuality, etc.

Information is confidential when it is personal information given to someone who has a duty of confidence (the pharmacy staff) in the expectation that it will not be disclosed without the consent of the provider of the information.

Personal information may be known or stored on any medium. Photographs, videos, etc are subject to the same requirements as information stored in health records, on a computer, or given verbally.

**Keeping it confidential: following pharmacy procedures**

The following procedures have been put in place to support the confidential handling of information and should be followed by all staff:

* **Data Transfer SOP** (sets out the procedures around the secure transfer of data, collecting consent and maintaining confidentiality within the pharmacy including the use of safe havens);
* **Incident Management SOP** (sets out the procedures for responding to a security breach);
* Business Continuity SOP (sets out the procedures in the event of systems failure);
* **Portable Device and Bring Your Own Device (BYOD) policies and guidelines** (provides guidance for staff that use portable devices and removable media);
* **Access Control and Password Management SOP** (sets out procedures for the management of access rights to computer-based information systems).

Staff that have been issued with NHS Smartcards, and will have needed to state they will comply with the terms and conditions to enable Smartcard usage.

All staff need to ensure they are aware of the procedures that are relevant to their role and comply with them.

**Passwords, Smartcards and security**

All users will be assigned a level of access to the PMR system that is appropriate to their role. Personal passwords should be regarded as confidential and those passwords must not be communicated. Different password will be used for different systems, and suitable passwords should be set e.g. use of three random words as per advice from [National Cyber Security Centre (NCSC)](https://www.ncsc.gov.uk/blog-post/problems-forcing-regular-password-expiry). Some systems will require additional complexity.

No employee should attempt to bypass or defeat the security systems or attempt to obtain or use passwords or privileges issued to other employees. Any attempts to breach security should be immediately reported to your line manager or an IG lead.

**Use of email and web-based services**

Email and internet usage should be restricted to work related issues.

**Circumstances where confidential information can be disclosed**

The pharmacy will inform service users, staff and any other data subject why, how and for what purpose personal information is collected, recorded and processed – where required. This will be achieved by leaflets and information provided face to face during a consultation.

Personal information may be disclosed where the disclosure is necessary for healthcare purposes and is undertaken by a health professional or a person owing an equivalent duty of confidentiality. Consent may be implied or explicit.

Explicit consent of the data subject is required where a disclosure of personal information is not directly concerned with the healthcare / treatment of a service user e.g. medical research, health service management, financial audit, personnel data or where disclosure is to a non-health care professional.

Explicit consent may be given in writing or verbally. A basic explanation of what information is to be disclosed and why / what further uses may be made of it, must be provided to the data subject together with a description of the benefits that may result from the proposed sharing of information and any risks if consent is withheld.

Personal information may be disclosed without consent in certain circumstances, for example:

* Where required by law, for example prescribers must be notified where a patient presents a repeat prescription and the pharmacy becomes aware of clinically significant issues arising in connection with that prescription;
* Where permitted by law, for example where public interest overrides the need to keep the information confidential.

All requests for disclosure without the consent of the data subject, including requests from the police, should be referred to the pharmacy IG lead.

**Dealing with subject access issues**

Subject Access requests should be dealt with by [e.g. the pharmacist, IG lead etc]. In most cases, patients are not charged a fee. The requested information must be provided within one month of the request. The patient should be asked to provide their name, address, postcode and date of birth to ensure correct identification of the patient’s records. The patient request should be in writing. The patient should be asked to provide identification before the records are shared, for example their passport, full driving license, a credit card etc. The patient should be asked to either collect the information in person from the pharmacy or consent to the record being posted to them.

**Offsite/home/remote working arrangements**

Pharmacy staff and delivery drivers may take some information off-site such as when services will be performed for patients outside of the pharmacy building. Relevant staff will supervise documents and materials (including medicines) that may include patient identifiable information.

Other patient identifiable information must not be removed from the pharmacy.

In regard to pharmacy-related information excluding patient identifiable information:

* This would normally be processed within the pharmacy.
* Information may be removed for home working purposes if required, if senior staff support this (although this would usually not extend to processing of clinical information unless mitigations are put in place e.g. virtual private networks (VPNs) to protect data being processed digitally).
* Generally information worked on from home is better to access digitally if possible. Paperwork might be at risk of being physically stolen. If paperwork does require to be taken out of the pharmacy it might be placed within an envelope or folder and labelled with advice to ‘contact person x if found’.

Patient identifiable information should never be left within vehicles overnight or for long periods in which the vehicle is unoccupied.

Within the home, a separate allocated room or workspace should be used for remote working, where possible so that pharmacy-related information is less likely to become misplaced.

Mobile computing and Bring Your Own policies will apply.

Connectivity via WiFi or mobile data contracts will be the responsibility of the device owner. Digital information must only be downloaded or uploaded over a secure connection. It must not be downloaded over a public WiFi network because of the lesser security within public WiFi networks e.g. avoid downloading sensitive information using public WiFi from airports, hotels, coffee shops, public transport etc.

**Support**

For assistance with disclosure issues, please contact the pharmacist or Information Governance lead.

**Abuse of privilege and breach of confidentiality**

It is strictly forbidden for employees to look at information about any patient including any information relating to their own family, friends and acquaintances unless they are directly involved in the patient’s care or with administration on behalf of the pharmacy. Action of this kind will be viewed as a breach of confidentiality and may result in disciplinary action.

**Possible sanctions for breach of confidentiality**

Breach of this code could lead to disciplinary action. Depending on the circumstances this could range from remedial training to dismissal. Prosecution or an action for civil damages may also be taken under current data protection legislation.

|  |
| --- |
| *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* |