

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| < Insert name of pharmacy>  **Access control and password management 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)*.* |  |

Technical access controls are built into information systems by pharmacy IT system suppliers. To ensure data is safeguarded, this functionality must be complemented by operational and managerial controls put in place in the pharmacy. This document outlines the procedures for managing access to systems. This procedure provides guidance on how staff access to the Patient Medication Record system is managed.

**Authorising access to the system**

## The following individual(s) are responsible for ensuring all the staff in the pharmacy have appropriate access rights to the system where required: <Add names e.g. IG Lead, Pharmacist in charge>

<Add details of the technical access controls built into the system, for example role-based access profiles. Contact your system supplier as necessary for more information.>

*Note regarding clinical systems*: Wherever possible, all users should be assigned an individual user ID and password with the access level set at the lowest level possible that still permits the staff member to undertake their role. However, there is a balance between security and usability of systems and it is recognised that individual staff logins may not be always be a practical option at this time, for example to control access to the PMR system by pharmacy staff. Decisions on the extent of access controls applied should be taken by the pharmacy contractor based on the risks of unauthorised access, the nature of the data and the impact on pharmacy workload of any controls. In some cases use of the pharmacy systems is already limited to the geographic location of the PMR terminal.

**Password policy, good practice and tips**

Passwords will not be reused for multi systems in case of a breach in which a password is exposed by a bad actor.

Staff will create strong and memorable passwords e.g. three random words, e.g. ‘planeyellowbread’, although some systems will require additional complexity (e.g. capital letters, numbers or punctuation). Regular password change is not required unless the system demands. National Cyber Security Centre (NCSC) now recommends organisations do not force regular password expiry because they indicate that can increase the risk of workarounds. Read more: [NCSC password information](https://www.ncsc.gov.uk/articles/problems-forcing-regular-password-expiry).

## **Password tips**

Summary tips for staff to be aware of are set out below.

* **Three random words**: Three random words are recommended by NCSC although some systems will require additional complexity.
* **Dictionary attacks**: Avoid consecutive keyboard combinations— such as ‘qwerty’, ‘asdfg’, ‘123456’ or ‘111111’.
* **Avoid using personal information within security questions**: You may be able to set-up security questions and answers but be cautious of including any information available online or within your social media. This protects you from bad actors being able to take control of your account using the ‘forgotten password’ and ‘security questions’ options.
* **Simple passwords**: Do not use information such as your name, age, birth date, name of loved ones, pet’s name, or favourite colour/song, etc.
* **Don’t reuse of passwords across multiple sites**: Reusing passwords for multi accounts can lead to one breach of your credentials posing a greater threat.
* **Make sure you use different passwords for each of your accounts**.
* **Be sure no one watches when you enter your password**.
* **Avoid entering passwords into computers you do not control** (e.g. internet cafés or libraries)—they may ‘auto remember’ your password or even have malware that steals passwords.
* **Avoid entering passwords when using unsecured Wi-Fi connections** (e.g. airports or coffee shops)—hackers can intercept your passwords and data over this unsecured connection.
* **Don’t tell anyone your password**. Your trusted friend now might not be your friend in the future. Keep your passwords safe by keeping them to yourself.
* **It’s okay to write down your passwords and keep these safe**, just keep them away from your computer and mixed in with other numbers and letters so it’s not apparent that it’s a password.

**Managing changes to access rights**

## **A. Joiners**

As part of normal induction processes new staff required to use the computer system will be issued with a username, password and access rights appropriate to their role. Joiners may have the pharmacy ODS code added to their Smartcard and may have a personal account linked to the shared pharmacy mailbox. New joiners should also receive data security training upon their arrival and at least annually thereafter (see [psnc.org.uk/dstraining](https://psnc.org.uk/dstraining)).

## **B. Profile changes**

Whenever there is a temporary or permanent significant change in the way a person works, a review of their access rights must be carried out.

## **C. Leavers**

When staff members leave permanently, their profiles and IT rights should be removed.

This may include:

* The removal of the ODS from their Smartcard – which can be done remotely by the local Smartcard Registration Authority (RA) – by the leaver or the pharmacy or both.
* If the staff member had their NHSmail personal account linked to the shared pharmacy NHSmail account, the pharmacy owner may unlink the staff member’s personal account.

## **D. Locums**

<Add local process for management of locum accounts>

## **E. Forgotten passwords**

Any staff member who has forgotten their password should contact ……………………… <add name e.g. IG Lead>

## **F. Misuse**

If any staff member suspects misuse for example if their password has been accidentally disclosed, this must be reported to……………………………… <add name e.g. IG Lead/pharmacist in charge>. Depending on the severity of the allegation an investigation maybe required and appropriate disciplinary measures taken.

**Procedures for staff in relation to logging in to the system**

*Note: Any relevant procedures, for example if passwords must be changed after first login, if a particular complexity of password must be used, if passwords must be changed periodically, if the system prevents password re-use, if the user can change their password at their request etc.*

**Local audit**

The management of access rights will be subject to internal audit to ensure that this procedure is being followed. The audit will be undertaken every 6 months and will be co-ordinated by <add name e.g. IG lead, sponsor etc>. Areas considered in the audit:

* Are only staff regularly working in the pharmacy registered as active users on the system.
* Is there any evidence of staff sharing their access rights?

DSPTK Template 13: ‘Audit checklist for spot check’ may also be used (see [psnc.org.uk/dstemplates](https://psnc.org.uk/dstemplates)).

***Note: Maintaining data security during ongoing pandemics****: It is recommended during ongoing pandemics that any audits being conducted by staff not usually working within the pharmacy building, are conducted remotely e.g. by phone call(s), email(s) and video meeting(s). Data security can be maintained remotely during or after pandemics.*

**Requirements for periodic review of the document**

The procedure will be reviewed annually taking into consideration changed in national guidance and changes made to the technical access controls in systems by pharmacy system suppliers.

|  |
| --- |
| *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* |