

## Information Governance - Introduction

Information Governance is the way by which the NHS handles all organisational information – in particular the personal and sensitive information of patients. It allows organisations and individuals to ensure that personal information is dealt with legally, securely, efficiently and effectively, in order to deliver the best possible care.

The principles of information security require that all reasonable care is taken to prevent inappropriate access, modification or manipulation of data from taking place. In the case of the NHS, the most sensitive of our data is patient record information.

In order to help you meet aspects of the Patient Care Record Guarantee, Pharmacy Manager keeps a record of everyone who was logged in (using their password) or logged out at any particular time.

This information can then be compared with the event dates and times in a [patient's history](#) to determine who the logged in user at any point was in time.

To prevent unauthorised access to confidential patient data, ideally, all pharmacy users should be assigned an individual user ID. However, there is a balance between security and usability of system, and it is recognised that individual staff logins may not be a practical option at this time, for example to control access to Pharmacy Manager by your pharmacy staff. This access control and reporting functionality is likely to develop over time as it is linked to work being carried out by NHS CfH.

Decisions on the extent of access controls 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.

Pharmacy Manager provides password protection in line with suggestions from the NHS Information Governance Pharmacy Contractor Workbook (Requirement 305 - page 28) Users must change their password after the first log in.

- Users must specify complex passwords.
- Users must change their passwords periodically.
- Prevention of password re-use.
- Users may change their password at their request.

A temporary administrator password is supplied as part of the installation/upgrade. This remains valid for 28 days during which period it is advised that you create your own user ID/passwords.



If you do not enter at least one administrator password within the first 28 days following installation/upgrade, access to Pharmacy Manager is disabled and can only be gained with assistance from the Service Desk.

It is suggested that the IG lead input a list of users (including themselves) with user IDs and temporary start-up passwords that require each individual to change them when first used. The IG lead does not need to consult with staff in determining user IDs as the system creates them automatically from the entered first and last names.

Similarly, as part of any normal induction processes new staff required to use the computer system should be issued with a user ID, password and access rights appropriate to their role.

## Adding user accounts

For England EPS R2 configured systems, user accounts can be added to enable all your staff to have access to Pharmacy Manager. The level of security is a Connecting for Health requirement. Use of this feature will maintain an audit trail of who logs in and out of Pharmacy Manager.

There are two types of account, Administrator and User:

Administrators can:

- Add, disable and delete user access accounts
- Reset Passwords
- Force change of password
- View other user details
- Access Pharmacy Manager

Users can:

- Access Pharmacy Manager

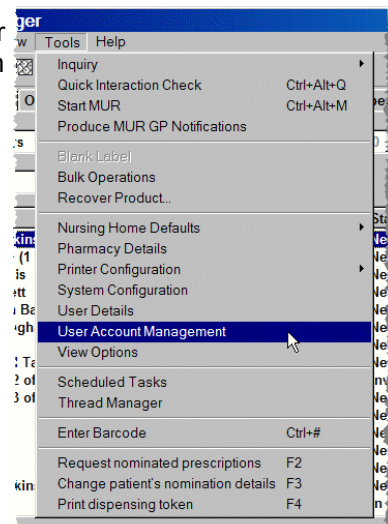
It is advisable to have more than one administrator to ensure any issues can be resolved at any time the pharmacy is open. Similarly, it is recommended that your Information Governance Lead should be an administrator.

As an administrator, click Tools and select User account management from the drop-down menu.

When logged in as a User, (not as an administrator) the User account management feature is not available on the drop down menu.

When the Pharmacy Manager Information Governance functionality is first enabled, a temporary user account ID with a default password is used to access the system. Details of this temporary account will be provided by the Cegedim Rx Support analyst enabling the functionality.

This account has the permissions of an administrator which will enable all users to be entered onto the system. It is temporary and only lasts 28 days following activation. If you are still using this after 24 days have elapsed, you will receive warnings that, unless you create your own administrator account, you will be blocked from using the system as the temporary user account will be deleted.



Once a new administrator account has been added, the temporary is automatically removed. In the event that this happens, please contact Service Desk for assistance in creating a new administrator password.

Click the Add button.

An empty User details screen appears.

Add in the detail that is required, noting that several options are mandatory.

Only check the Administrator account a check box if the user is to be given Administrator level access.

### First and last names

Enter your first name and last name. The first name can be your initial.

The first letters of each are capitalised automatically by Pharmacy Manager.

Your username is derived from the first name and last name e.g. Alan and Beech will create "ABeech" as a username. Each username features two upper case characters as the first two letters. These must be typed correctly when subsequently logging in.

### Job role

It is recommended that you can record a job role against each user.

### Professional reference

Type in your RPSGB registration number

### Password

Enter a password. The password entered at this point will only be valid at the very first log in for this user. They will be forced to create their own password.

The password will be case sensitive, so whether letters are upper or lower case must be remembered.

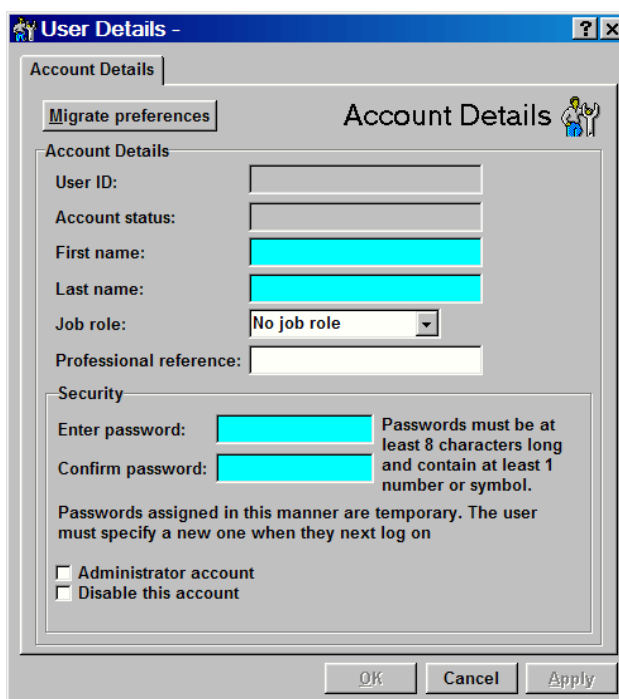
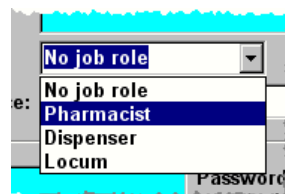
To ensure satisfactory password strength, the password must also meet minimum criteria:

- be at least 8 characters long
- contain either at least one number (0-9) or one symbol e.g. ! £ \$ % & \* # @

If a password is forgotten, any administrator can trigger a password reset to allow the selected user to enter a new password.

### Administrator account

Check  the Administrator account box if this user is to have administrator privileges. This would enable them to reset forgotten passwords.

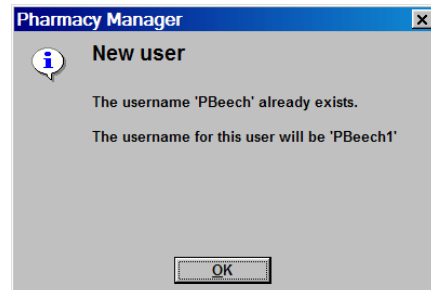



Check  the Disable this account box to suspend the user ID.

When all the necessary detail has been added, click the OK button to save the user account addition and to exit.

### Duplicated user ID

If you attempt to create a new user account for a user who shares first name initial and last name with a current user, the new user ID will be automatically adjusted by the addition of a number at the end.

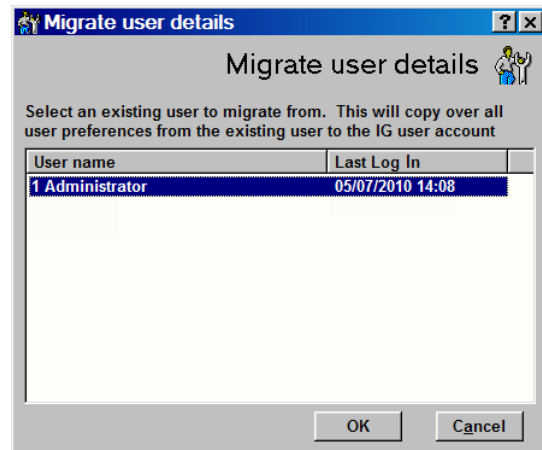


### Migrate preferences

It is advisable to use the "migrate preferences" button to ensure that each user has the same configuration of Pharmacy Manager. If you choose not to migrate the preferences, there is a potential for each user to have a different configuration for settings such as Endorsing and dispensing order.

If you wish to migrate customised user details to a new user account, click the Migrate button.

Select the user from whom you wish to migrate their user details. Typically, there will only be one choice. However, if there are more, the likely selection is going to be Administrator.



Click the OK button to confirm your choice.

## User account management

Once an account has been created, you may be required to make changes.

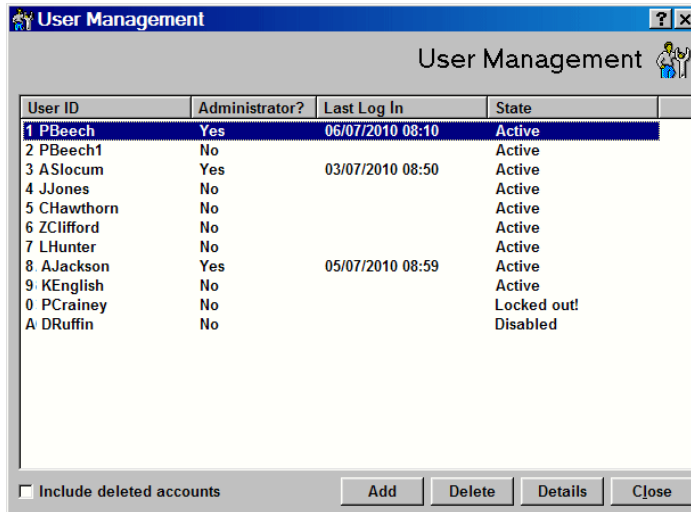
As an administrator, click Tools and select User account management from the drop-down menu.

A list of existing user accounts is displayed. The columns include the User ID, whether the user is an administrator or not, when they have last logged in to Pharmacy Manager and their account state.

The account state will normally indicate Active. However, other states may appear from time to time.

Locked out - this user has exceeded the permitted number of invalid incorrect attempts to log in. An administrator can set a new temporary password to enable the user to log in.

Disabled - an administrator can prevent any user from logging in by disabling a user account.



| User ID     | Administrator? | Last Log In      | State       |
|-------------|----------------|------------------|-------------|
| 1 PBeech    | Yes            | 06/07/2010 08:10 | Active      |
| 2 PBeech1   | No             |                  | Active      |
| 3 ASlocum   | Yes            | 03/07/2010 08:50 | Active      |
| 4 JJones    | No             |                  | Active      |
| 5 CHawthorn | No             |                  | Active      |
| 6 ZClifford | No             |                  | Active      |
| 7 LHunter   | No             |                  | Active      |
| 8 AJackson  | Yes            | 05/07/2010 08:59 | Active      |
| 9 KEnglish  | No             |                  | Active      |
| 0 PCrainey  | No             |                  | Locked out! |
| A DRuffin   | No             |                  | Disabled    |

Include deleted accounts
 Add
Delete
Details
Close

Click the Add button to append a new user.

Click the Delete button to remove the highlighted entry from the visible list. For audit purposes the deleted user account is retained in the system. Check Include deleted accounts for any such users to be displayed as well.

In the event that an account is inadvertently deleted, an administrator can edit and re-instate a deleted user account.

Click the Details button to view the current settings for the selected user.



**Account Details**

Migrate preferences

Account Details

User ID: PHerne

Account status: Active

First name: Pamela

Last name: Herne

Job role: Pharmacist

Professional reference: 7676543

**Security**

Reset password: Force this user to create a new password next time they log in

Forgot password: Specify a temporary password to allow the user to log in. The user will then need to create a new password

Administrator account

Disable this account

OK Cancel Apply

### Reset password

An option exists that will enable an administrator to enforce the initial and, subsequently, the periodic renewal of passwords to maintain good system security.

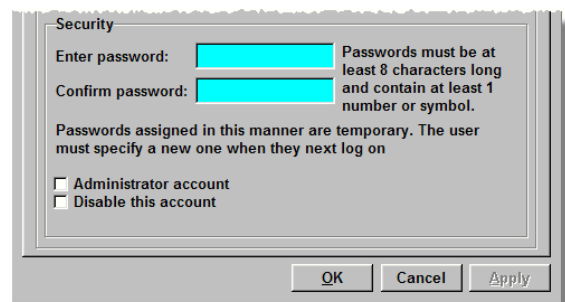
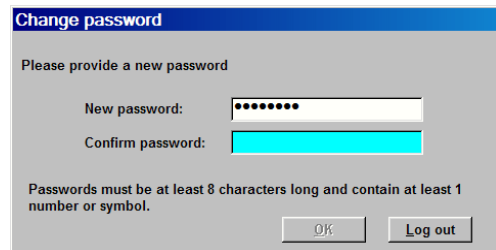
Click this button to trigger a password reset the next time the highlighted user tries to log in.

When users have to renew their passwords, they cannot re-use any of their last five passwords. An alert to this effect appears should any user try to recycle their passwords too frequently.

### Forgot password

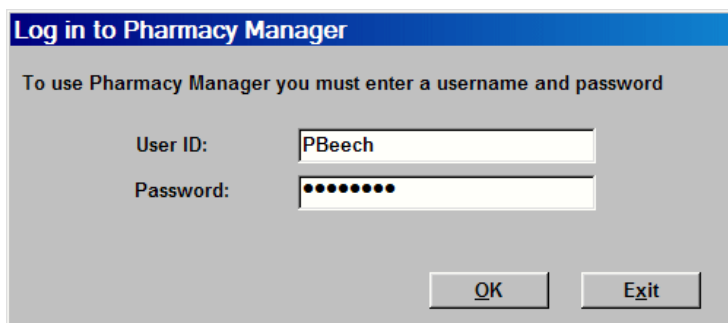
Click this button so that a temporary password can be specified. This will allow the user to log in next time in order to create a new password.

Enter a new password and re-enter a second time to confirm.



## Pharmacy Manager log in

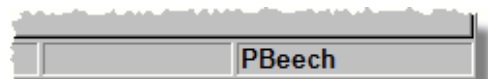
When you restart Pharmacy Manager, you are required to log in. Enter your username when the Log in prompt appears.



The first two letters of the user ID will be uppercase. The remainder is lowercase.

Enter your password and click the OK button.

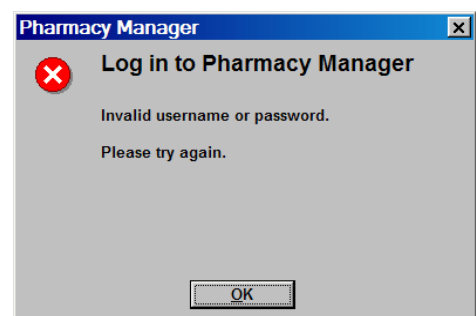
If the username and password have been typed correctly, Pharmacy Manager continues to load.



### Successful log in

Once you have successfully logged in, your user name is displayed at the bottom corner of the Pharmacy Manager display.

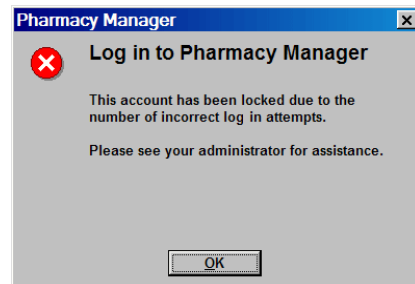
### Invalid password



### Failed attempts

After four failed log in attempts, a user will be locked out.

An administrator can force a new password reset, which will unlock the account.



### Pharmacy Manager log out

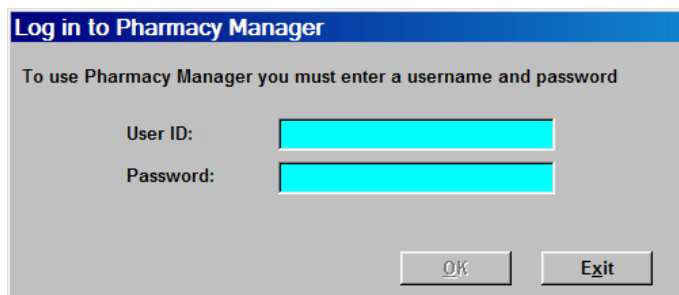
You can log out of Pharmacy Manager without closing down. For example, you may be leaving the premises and you wish to lock Pharmacy Manager in order that it is not used until your return.

Alternatively, your locum is going to log in during your absence.

Click the File option on the menu bar and select Log out.



An empty log in window appears prompting for the username and password of the person logging in.



Alternatively, you can click the Exit button to close down the system.

The OK button remains disabled until a username and password have been entered.

### Closing down

The action of closing down automatically logs the user out. If you click the Exit button, you will also be prompted to closedown Pharmacy Manager.

### Reports

There are reports available which will provide audit trails of who logged in and out of the system, and details of when user accounts were added, deleted, disabled and unlocked.

For more details, refer to the Help files within Pharmacy Manager.

## Next Steps

This checklist provides a list of the decisions and actions you must take before using the Information Governance functionality.

It is not exhaustive and you may choose to ignore some of the items, however the following details must be considered:

- **Once the functionality is enabled, every user must have a log in – this includes locums, even if they are only working at the store for 1 day.**
- **Failure to provide user login for every user will prevent use of the system**
- **Cegedim Rx cannot record or provide usernames and passwords, as it is in breach of Information Governance**
- **Cegedim Rx cannot create users, as it is in breach of Information Governance**

### Suggested action points:

- Determine the administrators

*Perhaps the IG Lead/s and the Pharmacist? An administrator should be available at all times.*

- Determine all other users

*This should be EVERYONE that will require access to the computer system*

- Determine your new user policy

*When will you add their details?*

- Determine your leavers policy

*Will you delete users when they will no longer be working at the store?*

- Determine your locum policy

*Will you delete a locum when they leave, or just disable them so they can be re-activated if they ever work with you again?*