Pharmacy Programs Administrator

PPA Portal MFA Support

1. What is multi-factor authentication (MFA)?

MFA is an extra layer of protection used to ensure the security of online accounts beyond just a username and password. It uses time-based verification codes to protect your login and the sensitive financial and patient information stored on the PPA Portal. The PPA is required to enforce MFA use on the PPA Portal for all users. New users will be prompted to turn on MFA as part of the registration process.

2. The PPA Portal is requesting a verification code. Where can I find the code?

You will find your verification codes on an authenticator app downloaded to your personal mobile device. Common authenticator apps include Google Authenticator and Microsoft Authenticator. Please note these apps are free to use and do not require payment or subscription. Once downloaded, most apps such as Google Authenticator and Microsoft Authenticator do not require internet access or use data to generate verification codes.

3. I cannot find my verification code on my authenticator app. Where are they?

Common scenario 1

Your mobile device may have multiple authenticator apps installed. Ensure that you have checked each one for a possible entry related to the PPA Portal (usually titled "PPA Online" with your login email). Some iOS users are prompted to use the "Passwords" app as their default MFA app.

Common scenario 2

If you have shared your login details with someone else, that person may have set up MFA for your login on their own mobile device. Follow the instructions in FAQ 4 to disable the MFA and reenable it correctly on your device. You should not share your login details with anyone.

4. Someone else set up MFA on my login to the PPA Portal. What should I do?

Request the other person provide you with a valid verification code from their device to access the PPA Portal. Then use these instructions to disable the MFA on the incorrect device and reenable it on your device:

1. Click your name in the top right of the screen, then click "Profile"
2. Click "Multi-Factor Authentication"
3. Click "Disable MFA" to disable the MFA link to the other person's device
4. Click "Setup authenticator app" to enable MFA on your personal device.

Please note that as MFA is mandatory; after disabling MFA you will need to enable it again prior to being able to continue using the PPA Portal with your account.

5. Can I share my PPA Portal login or MFA with a different person?

The PPA Portal allows multiple users to link to the same Service Provider. This means that every member of staff who needs access to the PPA Portal should use their own personal login. You should not share your login details with anyone.

6. I am employed at multiple Service Providers that use the PPA Portal. Can I use the same MFA/login for each Service Provider?

Yes, your MFA is associated with a single personal login account for the PPA Portal. This login can then be used to link to multiple Service Providers. For instance, a pharmacy owner can view and claim for several different Service Providers with one login.

7. What is a recovery code?

MFA authentication recovery codes are unique, one-time use codes that allow you to bypass the authenticator app if you lose access to it or your mobile device, providing a backup method to regain access to your PPA Portal login. Note that to use a recovery code, you must have already generated the recovery codes **before** being locked out and saved the codes in a secure location that does not require the use of your mobile device. Please see page 9 of the PPA Portal New User Guide for more information, linked here.

8. Can the PPA Support Centre provide MFA related assistance?

Yes, if you are having issues accessing the PPA Portal due to the MFA associated with your login please contact the PPA Support Centre from either a phone number or email address associated with your PPA Portal login.

9. Can the PPA Support Centre provide MFA assistance if I make contact on someone else’s behalf?

The PPA Support Centre can only provide specific advice to the owner of a login.