Provider Portal

How to log in to the Provider Portal

User Guide

Version 1 May 2025

xyla

Part of Acacium Group

1 Contents

2 Introduction

Working to the national digital specification the Provider Portal will enable ICB's to have an end to end digital solution for the CHC patient journey.

Our customers will have a more robust way of managing their providers, monitoring bed availability, improving financial governance and allow for improved document storage.

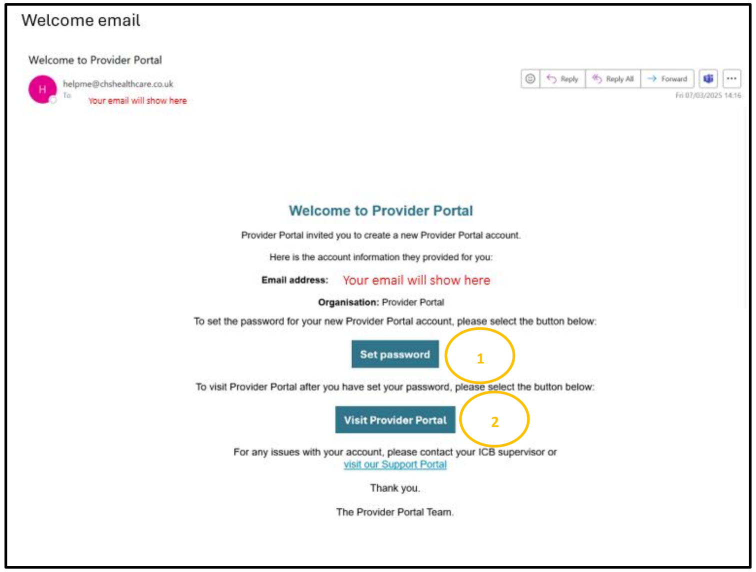
This short guide will provide you with guidance on how to login to the Provider Portal.

3 Logging in

Multi Factor Authentication (MFA) is used when logging into the Provider Portal as it adds a layer of protection to the sign-in process. Please download either the Google, or Microsoft Authenticator app on to your mobile device and then follow the below steps to set up MFA and log in to the Provider Portal.

Google Authenticator App   Microsoft Authenticator App

Once you have been provided with an account for the Provider Portal you will receive the below email.



Welcome email

Welcome to Provider Portal

helpme@chshealthcare.co.uk
To Your email will show here

Welcome to Provider Portal

Provider Portal invited you to create a new Provider Portal account.

Here is the account information they provided for you:

Email address: Your email will show here

Organisation: Provider Portal

To set the password for your new Provider Portal account, please select the button below:

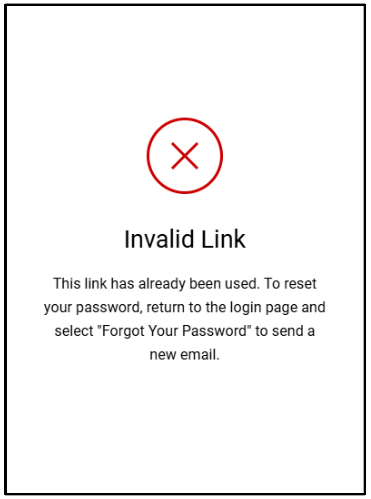
To visit Provider Portal after you have set your password, please select the button below:

For any issues with your account, please contact your ICB supervisor or visit our Support Portal

Thank you.

The Provider Portal Team.

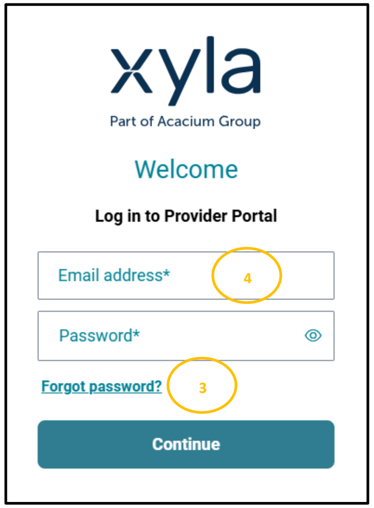
1. Click 'Set password'.
    - Please note the 'Set password' link will expire after 5 days. If you click 'Set password' after 5 days of receiving the 'Welcome' email the below message will appear, prompting you to select 'Forgot password' from your login page.
    - Please set you password before setting up MFA.



Invalid Link

This link has already been used. To reset your password, return to the login page and select "Forgot Your Password" to send a new email.

2. After you have set your password or if the 'Set password' link has expired click 'Visit Provider Portal' from your 'Welcome' email.
3. If your 'Set Password' link has expired, please click 'Forgot password?' and follow the instructions, once your password has been set click 'Visit Provider Portal' from the 'Welcome' email.
4. Enter your Email Address and Password and click 'Continue'.



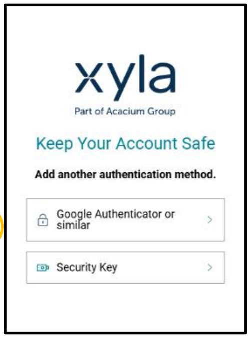
xyla
Part of Acacium Group

Welcome

Log in to Provider Portal

5. Please select ‘Google Authenticator or similar’.

   Google or Microsoft Authenticator Apps are both free to download and are completely safe to use on your mobiles.



xyla
Part of Acacium Group

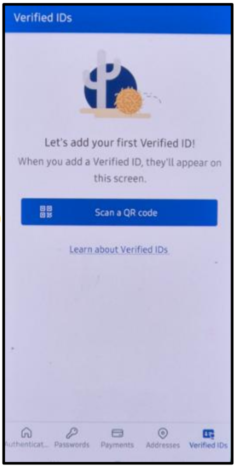
Keep Your Account Safe

Add another authentication method.

Google Authenticator or similar ›

Security Key ›

6. You will be presented with a QR code, open up your Google or Microsoft Authenticator App and click ‘Scan a QR code’, this will open up your camera from within your app.



Verified IDs

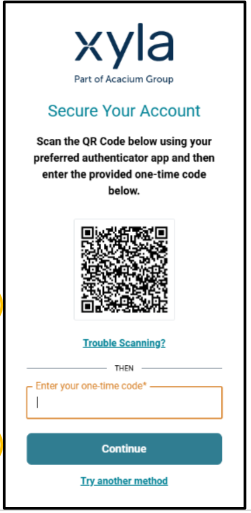
Let's add your first Verified ID!

When you add a Verified ID, they'll appear on this screen.

Scan a QR code

Learn about Verified IDs

7. Hover over the QR code displayed on screen, this will provide you with a One-time password code.
8. Enter the code provided into the box ‘Enter your one-time code’ on your laptop.
9. This will link the Provider Portal with your Authenticator App. Click on the Provider Portal line with your chosen authenticator app each time to retrieve your code, the countdown timer will reset every 30 seconds.



xyla
Part of Acacium Group

Secure Your Account

Scan the QR Code below using your preferred authenticator app and then enter the provided one-time code below.

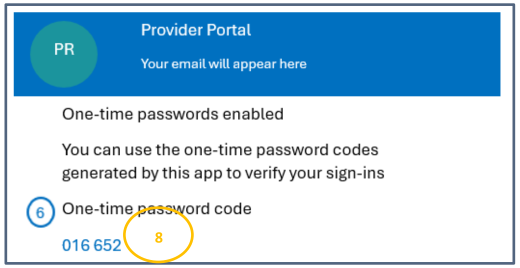
Trouble Scanning?

THEN

Enter your one-time code*

Continue

Try another method



PR

Provider Portal

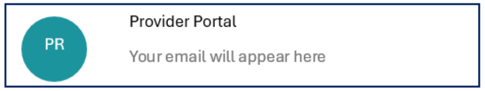
Your email will appear here

One-time passwords enabled

You can use the one-time password codes generated by this app to verify your sign-ins

6 One-time password code

016 652



PR

Provider Portal

Your email will appear here

Microsoft Authenticator App

1. Enter your Email Address and Password into the Provider Portal
2. Select Authenticator App and a QR Code will be displayed
3. Open up your Authenticator App
4. On the bottom right click on Verified IDs button
5. Click on Scan a QR code
6. This will open up your mobile camera from within the app itself
7. Hover over the QR code that is displayed on your laptop
8. This will link your Provider Portal access to your mobile device
9. Enter your Onetime code into the box on your laptop
10. You now have access

Google Authenticator App

1. Enter your Email Address and Password into the Referral Portal
2. Select Authenticator App and a QR Code will be displayed
3. Open up your Authenticator App
4. On the top right of the app click on the + button
5. This will open up your mobile camera from within the app itself
6. Hover over the QR code that is displayed on your laptop
7. This will link your Provider Portal access to your mobile device
8. Enter your Onetime code into the box on your laptop
9. You now have access

Please note: The QR will not be required again as MFA has been set up, you will only require your Email Address, Password, and One-time code found in your Mobile’s Authenticator App every 12 hours to access the Provider Portal.

4 Frequently Asked Questions (FAQ)

4.1 What is Multi-Factor Authentication (MFA)?

MFA is an additional way of checking that it is really you when you log in to your account. In addition to your username and password, you will need to set up another form of authentication such as using an authentication app on your smartphone or tablet. This second layer of security is designed to prevent anyone but you from accessing your account, even if they know your password.

4.2 What are the benefits of MFA?

- Keeps any patient data in a more protected environment
- Helps you gain access to your account should you forget your password
- Helps protect the reputation of the NHS
- Provides increased protection against cyber-attacks
- Checks if an attempt is made to access your account from an unusual location or device

4.3 I am getting authentication requests, but I am not trying to sign in. What should I do?

If you are not trying to sign in but you are receiving requests to approve a sign-in request or provide an authentication code, this indicates a malicious person is trying to access and compromise your account.

Only approve authentication requests when you know you are the one who made them. If you receive authentication requests that you have not made, do not approve them or select anything in the request. Alert your local IT team and protect your account by changing your password.

4.4 I have a new mobile phone but kept the same number. Do I need to do anything?

Firstly you will need to download the authenticator app on your new mobile phone. Then back up the details from your old mobile phone to your new one.

As MFA has been set up on your old mobile phone your MFA will need to be reset so you can follow the steps above and set it up on your new mobile phone.

Please raise this with the ICB lead and they will request for your MFA to be reset for you.

4.5 What should I do if my mobile phone is lost or stolen?

Inform your local IT team and remember to always register an alternative method of MFA for emergencies. You can do this by downloading an authenticator app on your new mobile phone.

As MFA has been set up on your old mobile phone your MFA will need to be reset so you can follow the steps at the start of the guide and set it up on your new mobile phone.

Please raise this with the ICB lead and they will request for this to be reset for you.

4.6 What if I do not want to use my personal mobile phone for MFA?

If you do not have a work mobile but want to use the Microsoft Authenticator app, we recommend you use your personal mobile. This is because it is unique to you. This helps ensure your account can only be accessed by you. Even if someone has your login details and password, they will not be able to log in to the Provider Portal without your personal mobile.

4.7 Can MFA allow data access to my personal mobile phone?

The Microsoft Authenticator app does not collect or store any personally identifiable data. Keeping your Provider Portal account secure and will protect the organisation, your own personal data, and patient data. Your personal mobile phone details are not used for any other purpose than protecting your account. By adding the Authenticator app to your personal mobile phone, you will just be providing a method to confirm who you are.

4.8 Does my mobile device need to be connected to the internet for MFA?

The Authenticator app uses a push notification on your phone to approve sign-in and this requires an internet connection.

4.9 Do I need to authenticate each time I log in to the Provider Portal?

Once you have logged into the Provider Portal and authenticated with a onetime code using MFA from you mobile phone you will then be authenticated for 12 hours. During this time period, you can log back in to the Provider Portal without needing to re-enter your login credentials or use MFA again.

Please reference the full Provider Portal guide for more information.