

# HSC Pharmacy Multi-Factor Authentication Set-up

MICROSOFT AUTHENTICATOR APP

*Prepared for*  
*Community Pharmacies*  
*Version 0.1*

*Prepared by*  
Noel O'Kane

Date: 25/07/2025

# Revision and Signoff Sheet

## Change Record

Date	Author	Version	Change Reference

## Reviewers

Name	Version Approved	Position	Date

## Terms & Abbreviations

Term/Abb	Meaning
HSCNI	Health and Social Care Northern Ireland
MFA	Multi-Factor Authentication
VDI	Virtual Desktop Infrastructure

## Table of Contents

Introduction .....	3
Audience .....	3
Pre-Requisites .....	3
Section 1 - Connect to VDI .....	4
Section 2 – Setup Using Microsoft Authenticator .....	10
Section 3 - Logging into VMS using the Microsoft Authenticator App (daily after set up) .....	17

# Introduction

The purpose of this document is to guide Community Pharmacists on the process of setting up Multi-Factor Authentication use the Authenticator App on an Android or iPhone.

## Audience

Community Pharmacies in Northern Ireland.

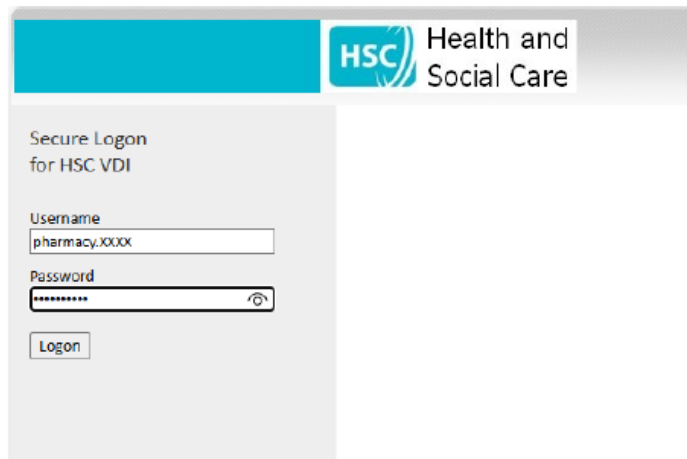
## Pre-Requisites

1. Pharmacy PC to log in to VDI
2. Access to Pharmacy / Vaccine email address
3. Microsoft Authenticator App downloaded from Google Play Store / Apple Store – other authenticator apps can also be used.
4. This must be completed with both your Pharmacy and Vaccine email addresses.

## Section 1 - Connect to VDI

1. Open Microsoft Edge and navigate to the below web address. The below screen will appear <https://vdi.hscni.net/portal/webclient/#/home>

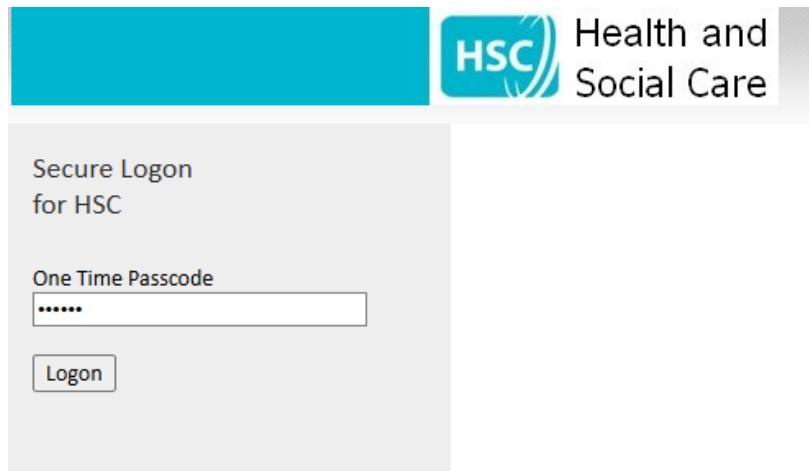
Login with your pharmacy or vaccine username. Eg **pharmacy.1234** or **vaccine.1234**. You do not need to put @hscni.net at the end of the username. The numbers correspond to your pharmacy contractor number.



The screenshot shows the 'Secure Logon for HSC VDI' interface. At the top, there is a blue header with the HSC logo and the text 'Health and Social Care'. Below the header, the title 'Secure Logon for HSC VDI' is displayed. The form contains two input fields: 'Username' and 'Password'. The 'Username' field is populated with 'pharmacy.XXXX'. The 'Password' field is masked with dots. A 'Logon' button is located at the bottom of the form.



The screenshot shows the 'Secure Logon for HSC VDI' interface. At the top, there is a blue header with the HSC logo and the text 'Health and Social Care'. Below the header, the title 'Secure Logon for HSC VDI' is displayed. The form contains two input fields: 'Username' and 'Password'. The 'Username' field is populated with 'vaccine.XXXX'. The 'Password' field is masked with dots. A 'Logon' button is located at the bottom of the form.



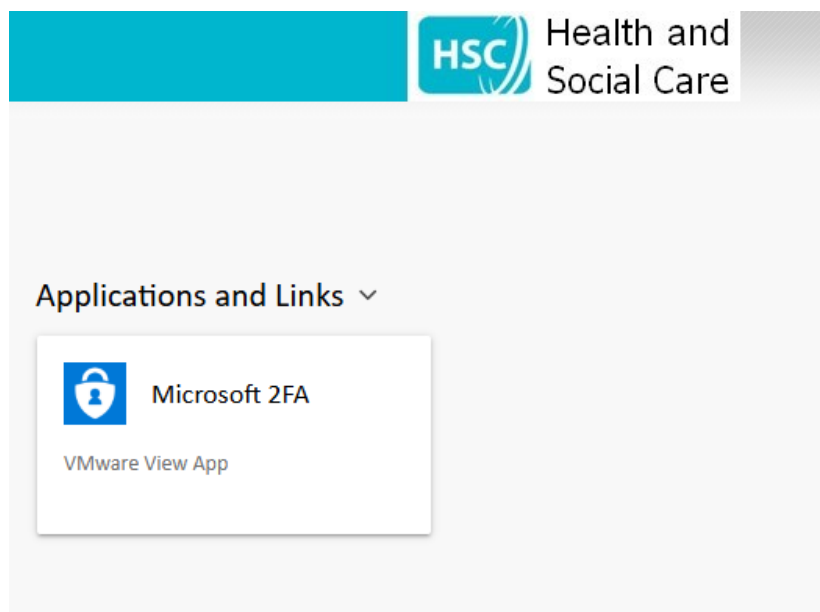
Secure Logon  
for HSC

One Time Passcode

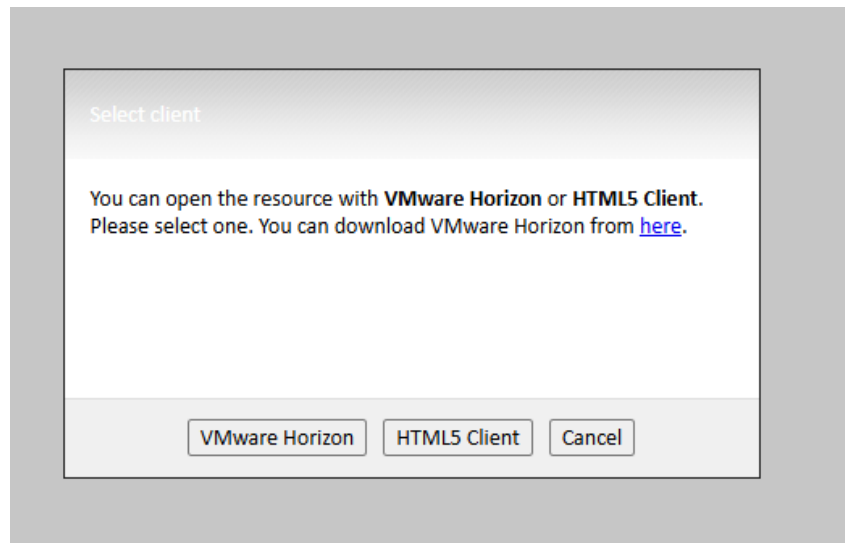
.....

Logon

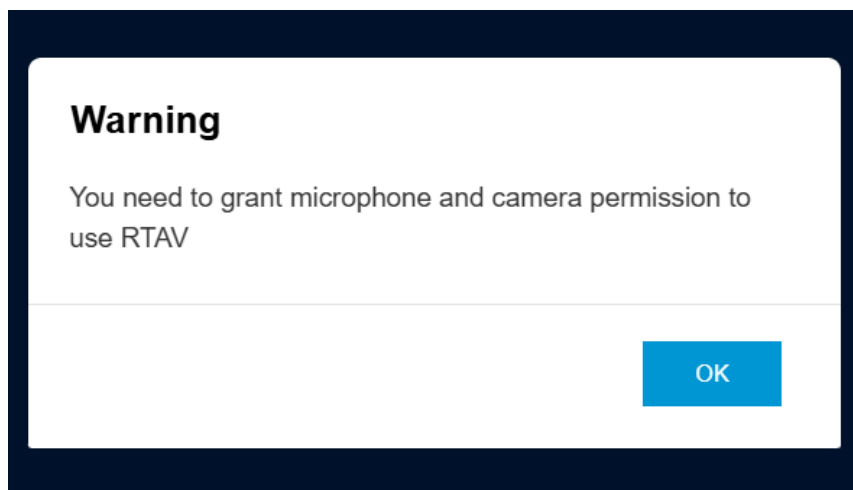
2. Log on to your [pharmacy.XXXX@hscni.net](mailto:pharmacy.XXXX@hscni.net) email address and you will have received a One Time Passcode, enter this in as shown in the above screenshot and click on Logon.



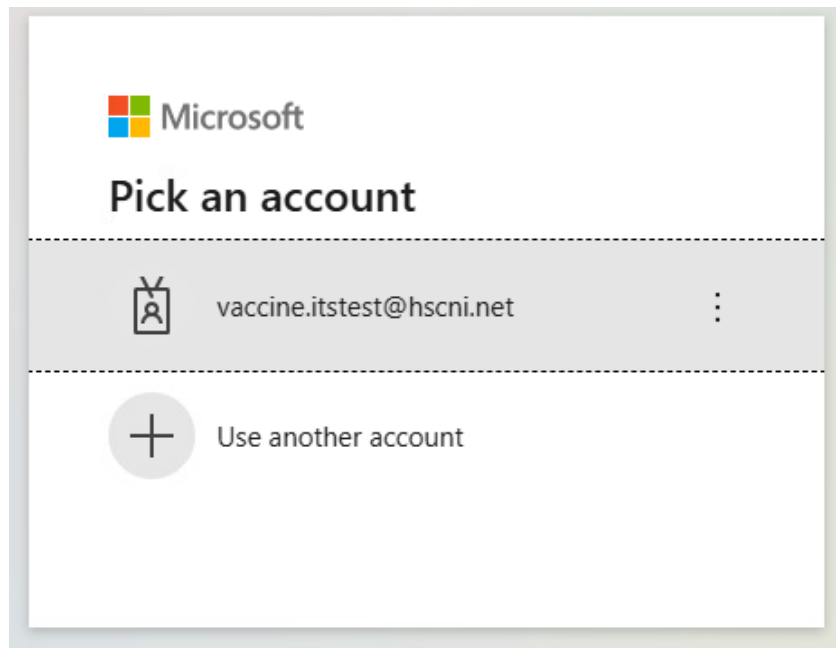
3. Click on the Microsoft 2FA box



4. Click on HTML5 Client – this opens the VMWare Horizon Web Application



5. If the above screen appears, click on OK. It may appear again on the top left-hand side of Edge, if it does click on Allow

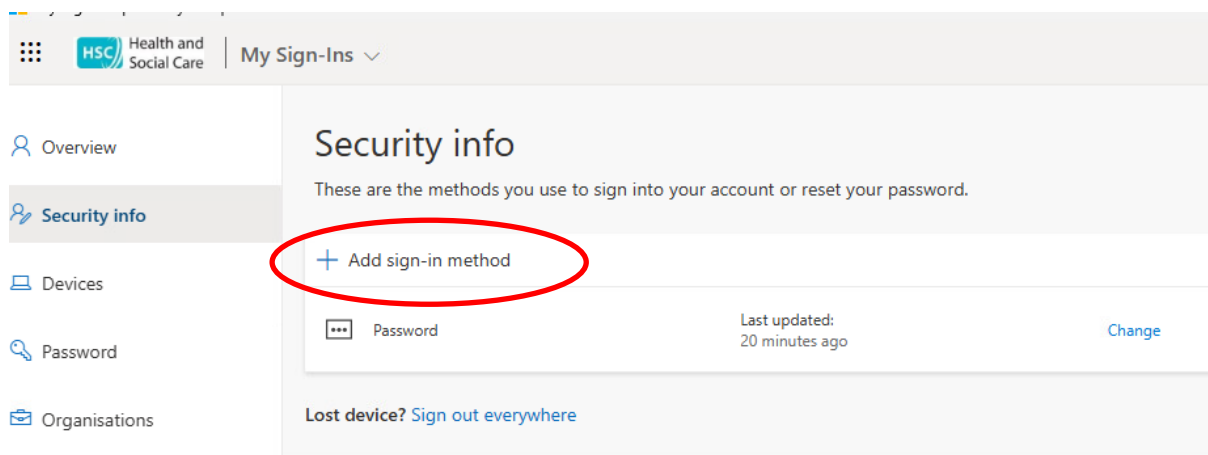
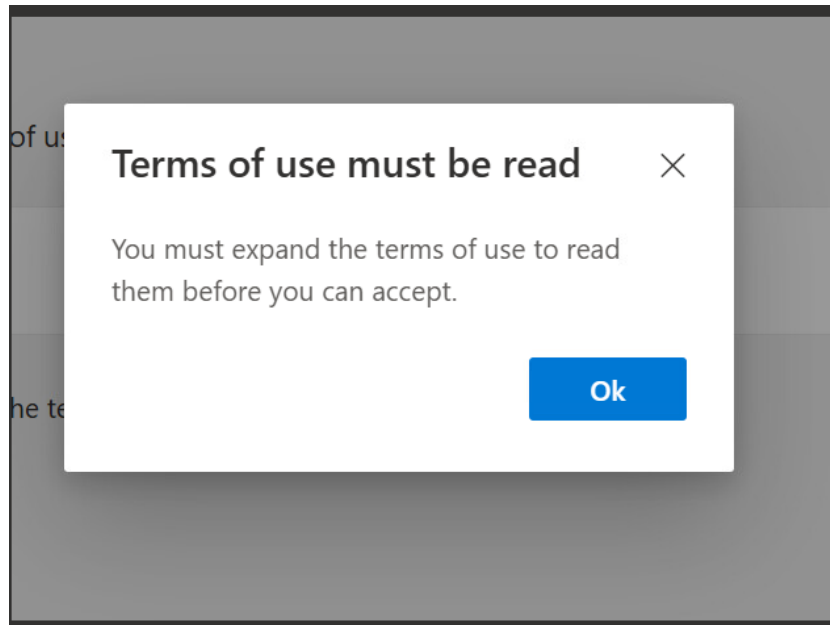


6. Click on your pharmacy/vaccine email – whichever one you have logged in to



7. You may be presented with a HSCNI Terms of use. You need to click on the arrow to the right of HSC Terms of Use and read the Terms of Use before Clicking on Accept. If you try to click on Accept you get the below screenshot.








8. Click on + Add sign-in method


Add a sign-in method

×

**Passkey in Microsoft Authenticator**  
Sign in with your face, fingerprint, PIN

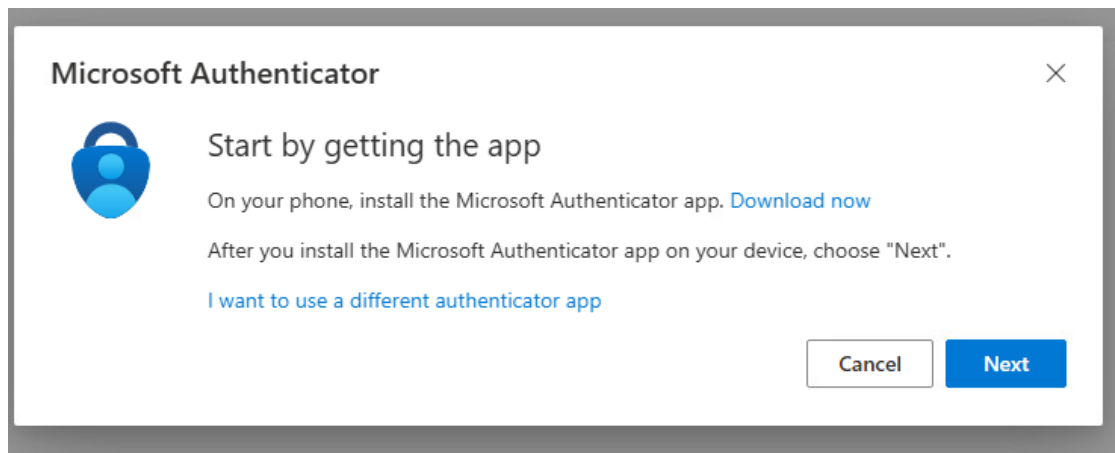
**Security key**  
Sign in using a USB, Bluetooth, or NFC device

**Microsoft Authenticator**  
Approve sign-in requests or use one-time codes

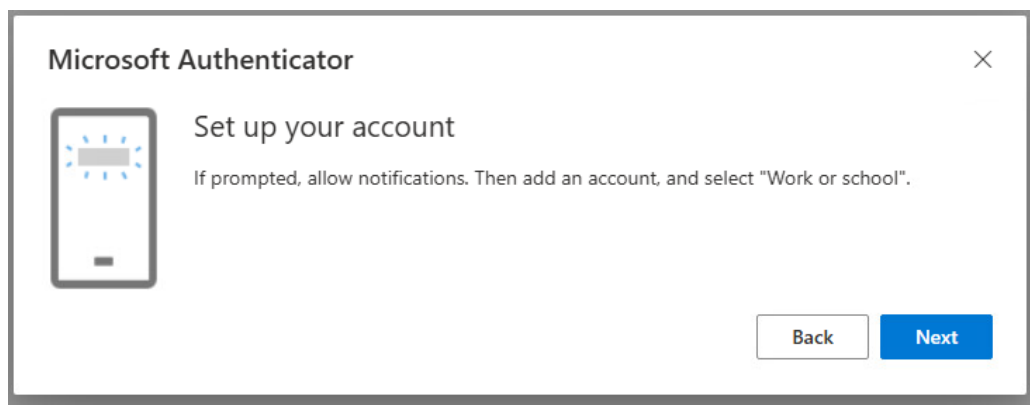
**Hardware token**  
Sign in with a code from a hardware token

9. Click on Microsoft Authenticator

## Section 2 – Setup Using Microsoft Authenticator



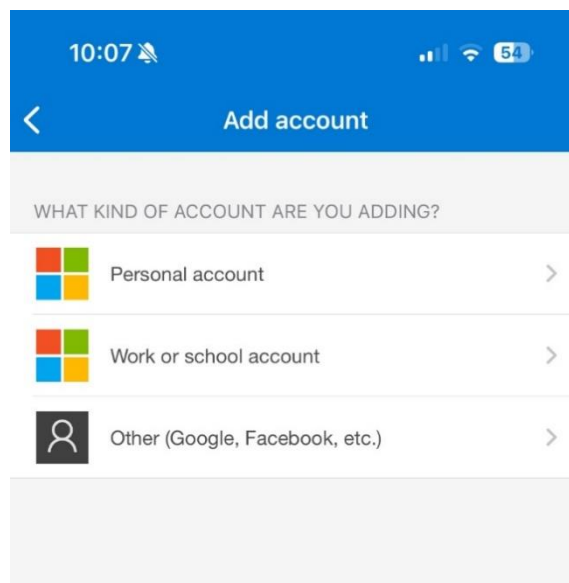
1. If using the Microsoft Authenticator App which is on an Android Mobile or Apple Mobile phone click on Next.



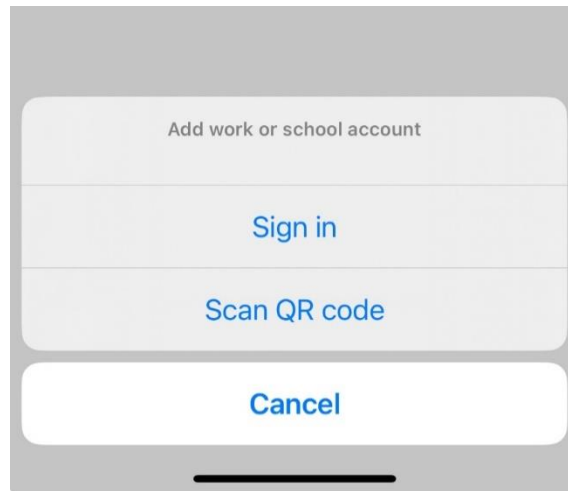
2. Click on Next



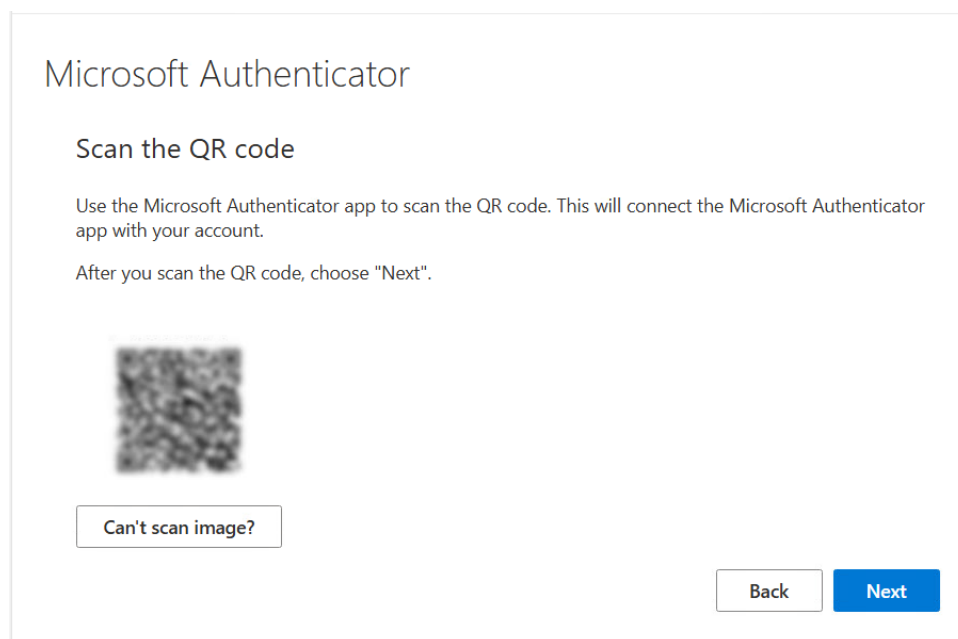
3. Open the Authenticator App on your mobile device and tap on the Plus symbol within the App



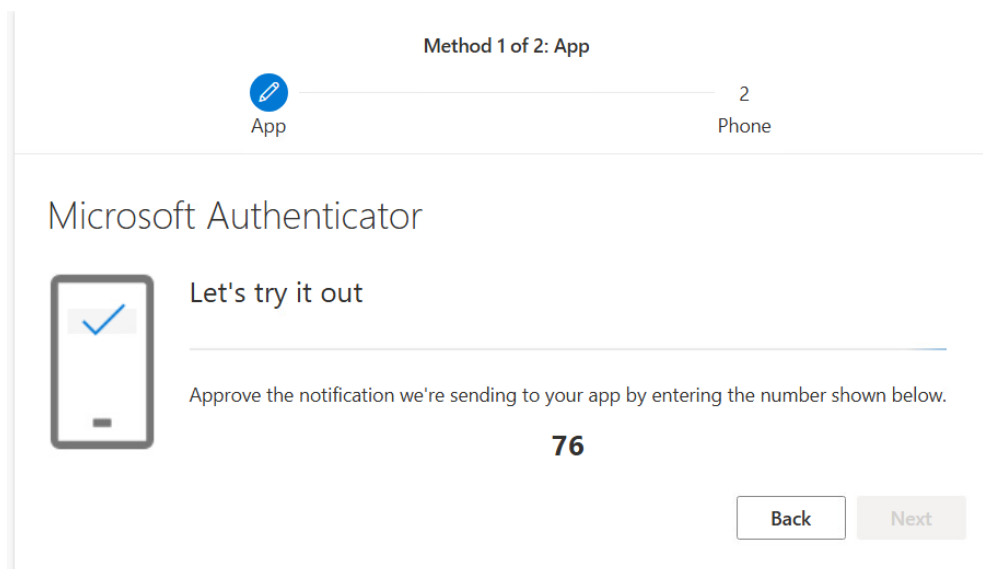
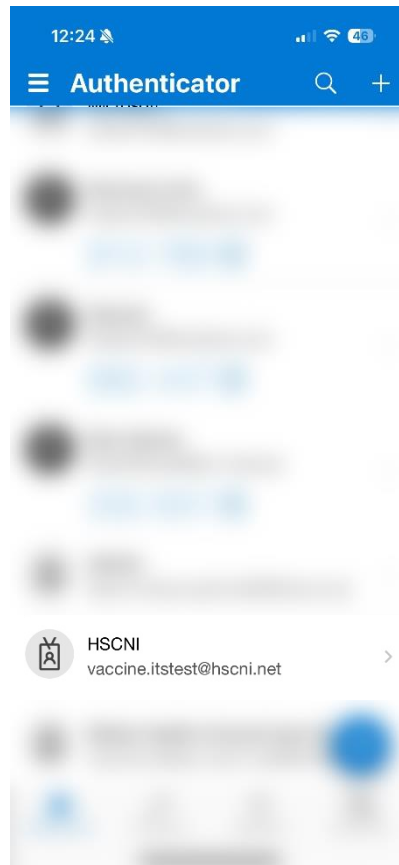
4. Tap on Work or school account



5. Tap on Scan QR code



6. Scan the QR code that appears on your own monitor, this will then add the Pharmacy or Vaccine account to the Authenticator App as seen on the below screenshot. Click on Next



7. The above screen then appears to test out the Authentication, a notification will appear on your mobile device and when you tap it, it will bring up the below screenshot asking are you trying to sign in.

**Are you trying to sign in?**  
HSCNI  
vaccine.itstest@hscni.net

Enter the number shown to sign in.

76



**No, it's not me** **Yes**

8. Input the number displayed on the PC Monitor and tap on Yes

Method 1 of 2: App

App 2 Phone

Microsoft Authenticator

  Notification approved

**Next**

9. Once authenticated the above screen appears. Click on Next

## Attaching Mobile Number to Authenticator App

You may be prompted to attach your mobile number to the Microsoft Authenticator App. This process will not be required if using a different Authenticator App on a Surface Pro/Tablet



The screenshot shows a 'Phone' setup window. It includes a close button (X) in the top right. The text reads: 'You can prove who you are by answering a call on your phone or receiving a code on your phone.' followed by 'What phone number would you like to use?'. There are two input fields: 'Country code' with a dropdown menu showing 'United Kingdom (+44)' and 'Phone number' with the text '7874342654'. Below these is a section 'Choose how to verify' with two radio buttons: 'Receive a code' (selected) and 'Call me'. At the bottom, there is a note: 'Message and data rates may apply. Choosing Next means that you agree to the [Terms of service](#) and [Privacy and cookies statement](#).' and two buttons: 'Cancel' and 'Next'.

1. Change country code to United Kingdom and put in your phone number minus the 0 at the start beside it. Ensure the Receive a code Radio button is selected and click on Next



The screenshot shows the same 'Phone' setup window, but now it's at a CAPTCHA step. The text reads: 'Please show you are not a robot.' Below this is a CAPTCHA image showing a blurry blue and white pattern. To the right of the image is a 'C' icon with a speech bubble. Below the image is a text input field with the placeholder 'Enter characters'. At the bottom are two buttons: 'Back' and 'Next'.

2. If prompted, enter in the characters that appear on your computer monitor and click on Next



## Phone



We just sent a 6 digit code to [redacted] Enter the code below.

536228

[Resend code](#)

Back

Next

3. Enter in the 6-digit number which you receive by Text Message and click on Next

## Phone



Verification complete. Your phone has been registered.

Done

4. Click on Done and your mobile number will appear as a Sign in Method as shown in the screenshot below

+ Add sign-in method			
	Phone	[redacted]	<a href="#">Change</a> <a href="#">Delete</a>
	Password	Last updated: 8 days ago	<a href="#">Change</a>
	Microsoft Authenticator Push multi-factor authentication (MFA)	Pixel 9 Pro	<a href="#">Delete</a>

## Section 3 - Logging into VMS using the Microsoft Authenticator App (daily after set up)

1. Navigate to <https://vms.healthandcareni.net/pharmacy>
2. Select Sign in
3. Enter your email address and select “Next”
4. Enter your password and select “Next”
5. A number will appear on your computer screen
6. A notification will appear on your mobile device asking to input the code that has appeared on your computer screen. Input this number and then tap OK.
7. The internet browser on the PC screens should automatically refresh and log you in to the Vaccine Management System.

If you have any issues with your Multi-Factor Authentication log a call with the BSO Service Desk for Attention of the Cloud Services Team – include as much detail as possible and any error messages you may be receiving.

**If you get a new Mobile phone or Tablet Device, you will need to log a call with the BSO Service Desk to get the Multi-Factor Authentication reset. You will then need to follow these instructions again to set it up again.**

Service Desk email address is – [supportteam@hscni.net](mailto:supportteam@hscni.net)