

1. On your mobile device, open the App Store or the Play Store and search for **Microsoft Authenticator**.



2. Install **Microsoft Authenticator** if it is not already installed.
3. On your computer, go to <https://aka.ms/mfasetup>
4. Enter your **HSC email address** and click **Next**.



Sign in

lobolouie@salud.unm.edu

[Can't access your account?](#)

Back

Next

5. Select **Work or school account** if prompted.



Work or school account
Created by your IT department
lobolouie@salud.unm.edu

6. Enter your **HSC NetID password** and click on **Sign In**.



← lobolouie@salud.unm.edu

Enter password

.....

[Forgot my password](#)

Sign in

7. Click on **Next** to provide more information.



lobolouie@salud.unm.edu

More information required

Your organization needs more information to keep your account secure

[Use a different account](#)

[Learn more](#)

[Next](#)

8. On **How should we call you?**, choose **Mobile app** from the first drop-down menu.



Additional security verification

Secure your account by adding phone verification to your password.

Step 1: How should we contact you?

A dark grey dropdown menu with three options: 'Authentication phone', 'Office phone', and 'Mobile app'. The 'Mobile app' option is highlighted with a blue background and a checkmark on the right side.

- ✓ Authentication phone
- Office phone
- Mobile app ✓

9. Select **Receive notifications for verification**.

A white rectangular box containing the question 'How do you want to use the mobile app?' and two radio button options. The first option, 'Receive notifications for verification', is selected with a blue radio button. The second option, 'Use verification code', is unselected with a white radio button.

How do you want to use the mobile app?

- Receive notifications for verification
- Use verification code

10. If you see a **Set Up button**, you may already have a device registered for MFA. Use the **Set up button** to renew the registration.

Use the instructions below as a guide.

Step 1: How should we contact you?

Mobile app 

How do you want to use the mobile app?

Receive notifications for verification

Use verification code

To use these verification methods, you must set up the Microsoft Authenticator app.

[Set up](#)

Mobile app has been configured.

11. Click **Next**.
12. A **QR code** should appear on your computer screen.
13. Grab your mobile device and open the **Microsoft Authenticator** app.



14. Tap **I agree** to consent to the privacy policy.



Your privacy matters

We collect required diagnostics to keep the app secure and updated. This does not include your name or any sensitive data.

I agree

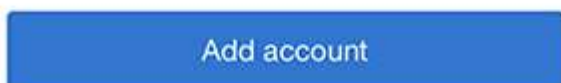
15. Tap **Skip** to continue.



Peace of mind for your digital life

16. Tap on **Add account**.

Ready to add your
first account?

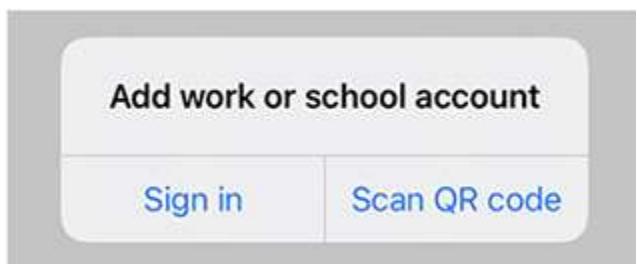


17. Tap on **Work or school account**.

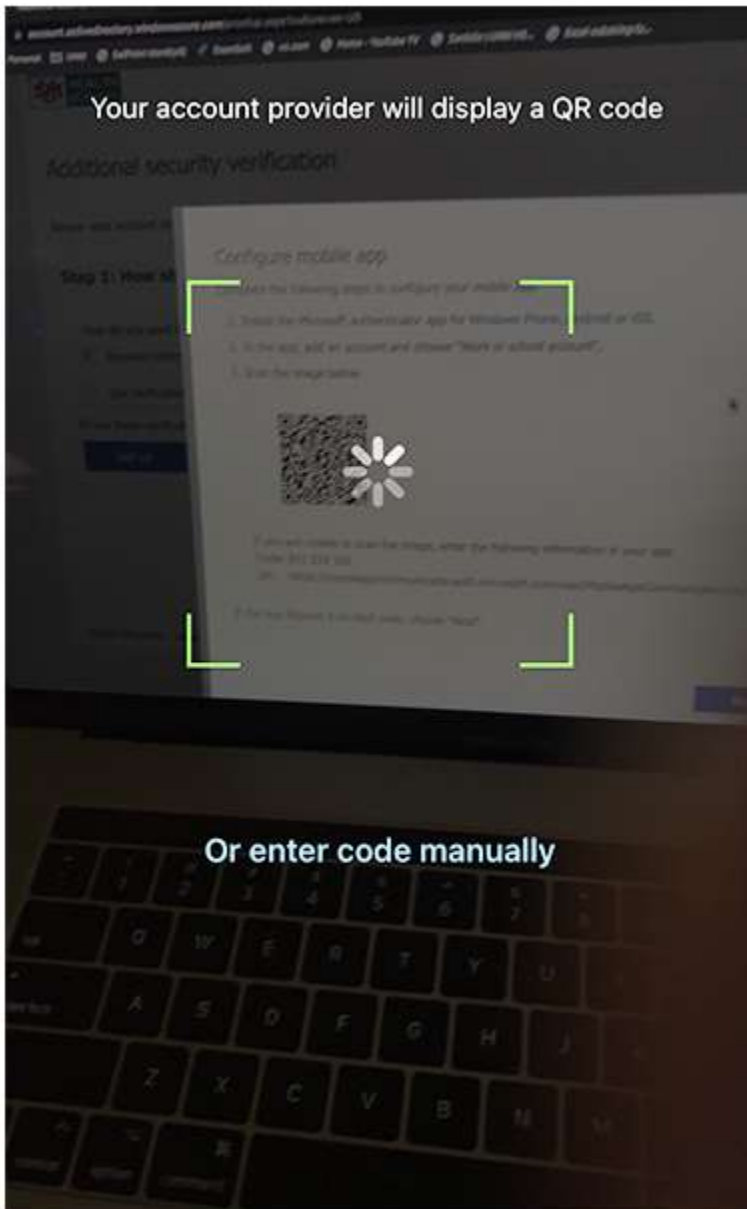


Work or school account

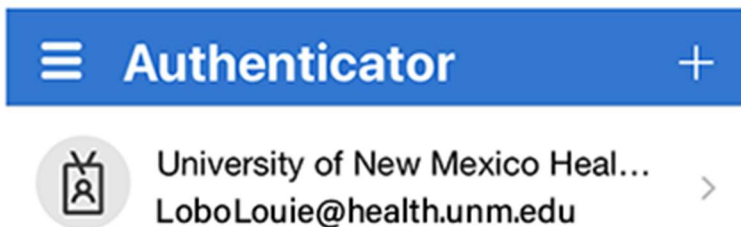
18. Tap on **Scan QR code**.



19. Point the camera at your computer screen to scan the **QR code**.



20. Your account will be added to the **Authenticator** app.



21. On your computer, click **Next**.

Step 1: How should we contact you?

Mobile app ▼

How do you want to use the mobile app?

Receive notifications for verification

Use verification code

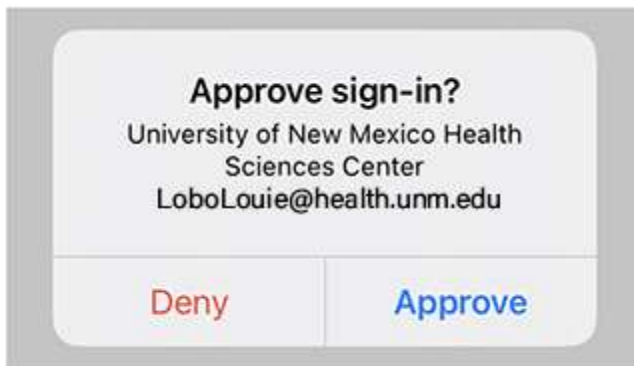
To use these verification methods, you must set up the Microsoft Authenticator app.

Set up

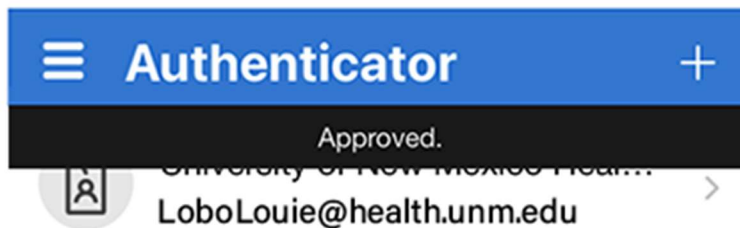
Mobile app has been configured for notifications and verification codes.

Next

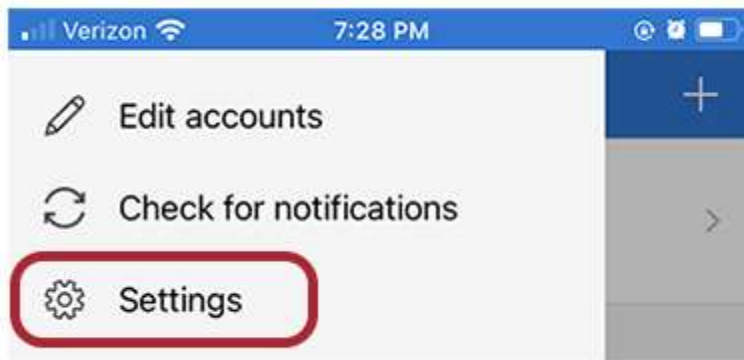
22. On your mobile device, tap **Approve**.



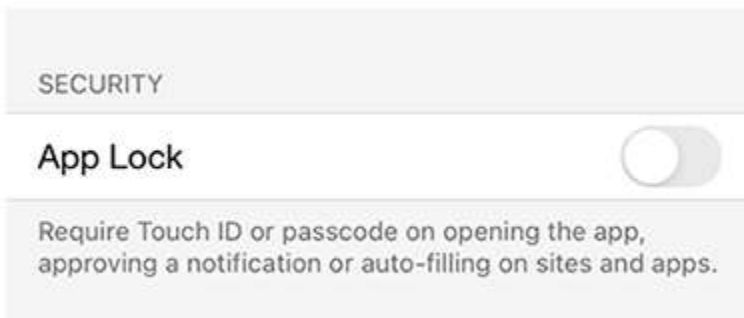
23. A black bar will pop up to confirm your selection.



24. Tap the **three stacked lines** in the top left corner (iOS) or the **three dots** in the top right corner (Android) and choose **Settings**.



25. Turn off **App Lock**.



26. On your computer, enter your **mobile phone number** and click on **Done**.

Step 3: In case you lose access to the mobile app

United States (+1)

Done

27. Decide if you want to add more ways of receiving MFA notifications, in case you temporarily lose access to your mobile device.

what's your preferred option?

We'll use this verification option by default.

Notify me through app ▼

how would you like to respond?

Set up one or more of these options. [Learn more](#)

<input checked="" type="checkbox"/> Authentication phone	* United States (+1) ▼	5051234567
<input type="checkbox"/> Office phone (do not use a Lync phone)	Select your country or region ▼	Extension <input type="text"/>
<input type="checkbox"/> Alternate authentication phone	Select your country or region ▼	

Authenticator app or Token [Set up Authenticator app](#)

Authenticator app - iPhone [Delete](#)

28. **Save** any new changes.

Congratulations! Your system is now ready for MFA. Please note that it can take several hours before you are prompted to MFA for the first time.

What to know about the MFA experience?

You will only be challenged for an 2nd factor when you are outside of the HSC network or in other words working remotely. When you are working and connected to the HSC network you will not be asked of

the 2nd factor to sign in. HSC Network in this document refers to the following: HSC_Secure, HSC_Guest, connected on site via an ethernet cable, or VPN-ed from off-site.