COLORADO
COMMUNITY
HEALTH
ALLIANCE

CCHA Provider Portal

Multifactor Authentication User Guide

For portal support, please email:

Portal@cchacares.com

CCHA Provider Portal – Setting up Multifactor Authentication

What is Multifactor Authentication (MFA)?

Multifactor Authentication, or MFA, is an extra layer of protection used to ensure the security of online accounts beyond just a username and password.

Why is MFA important?

The information housed on the CCHA Provider Portal is sensitive, containing protected health information (PHI) specific to your practice. Multifactor authentication provides an extra layer of security that protects not only your practice, but you as an individual. For this reason, MFA setup is required to access the CCHA Provider Portal.

What if I do not want to set up MFA?

If you do not set up MFA, you will **not** be able to log into the CCHA Provider Portal.

What If I get a new phone?

If you get a new phone for whatever reason, please alert your CCHA Provider Relations Network Manager or email Portal@cchacares.com.

ATTENTION: After October 26, 2022, the process to set up multifactor authentication will change. Please click on the option below based on today's date:

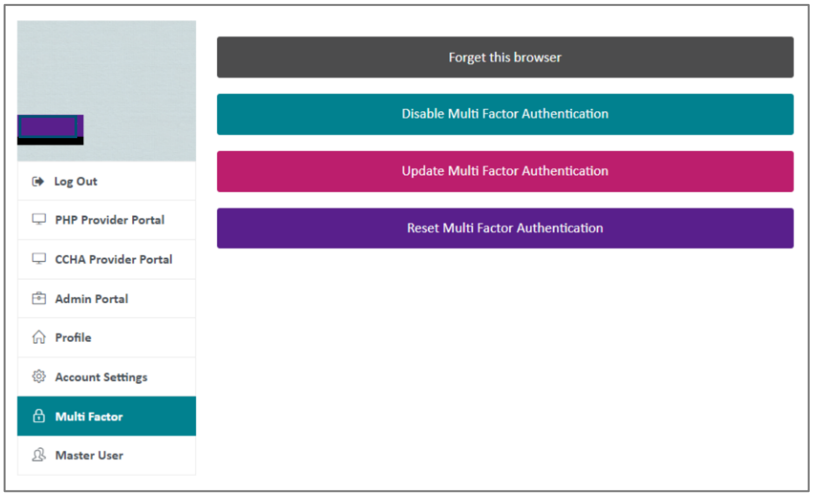
Before October 26, 2022

After October 26, 2022

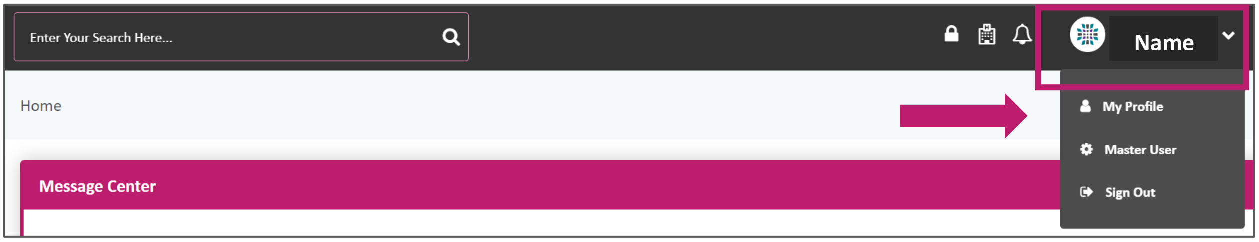
Starting October 2022, multifactor authentication is required for all CCHA Provider Portal accounts. You will not be able to access any information or resources on the portal without this security measure in place.

Setting up Multifactor Authentication BEFORE October 26, 2022

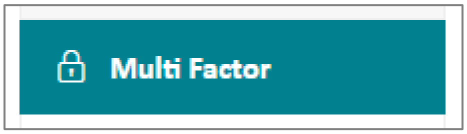
- Log into the CCHA Provider Portal, CCHAproviders.com.
- To set up MFA, you will need to be in *My Profile*.
    - If you log into a screen similar to the following, you are in *My Profile.*



- If you log into a screen similar to the following, you are in the *CCHA Provider Portal* and will not be able to see any data until you set up MFA.
    - In the top right-hand corner, click on your name to open the account management dropdown menu.
    - Click **My Profile**.



- Under My Profile, click **Multi Factor**.

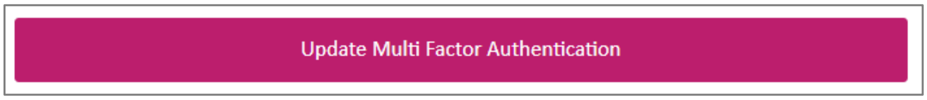


- You can also access Multifactor Factor menu options by clicking the **lock icon** in the top menu bar.

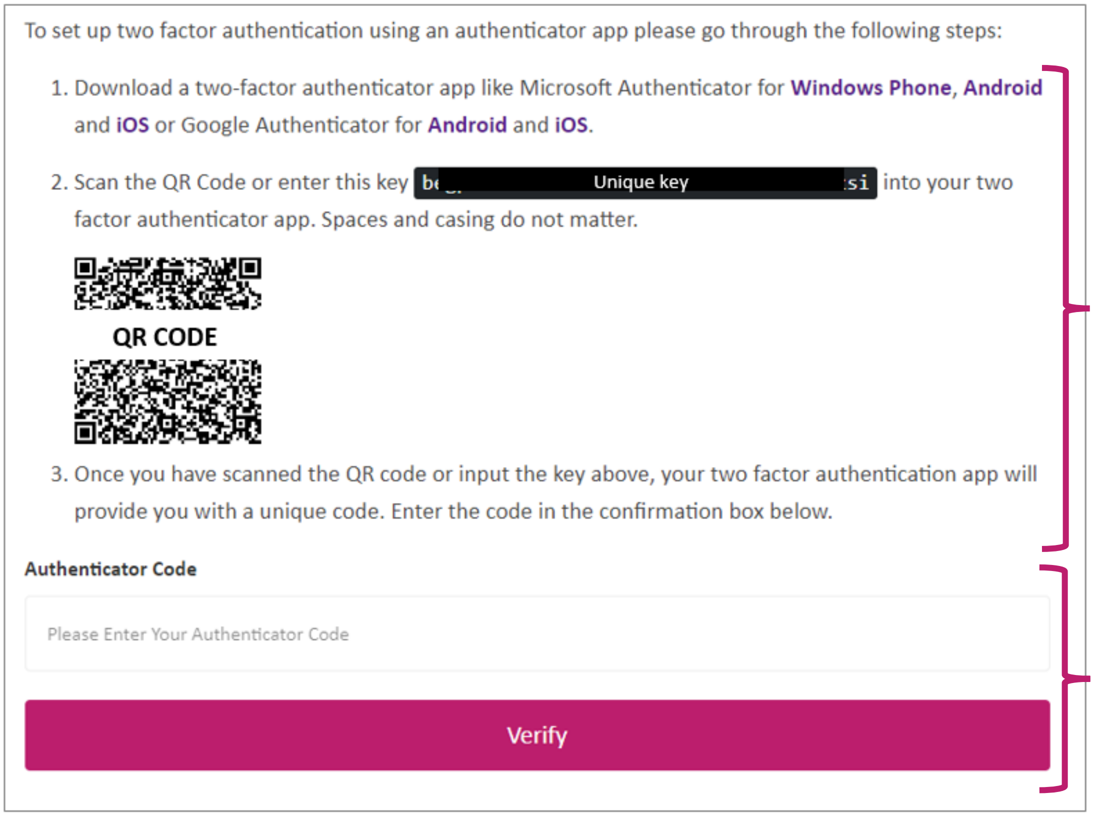
The lock icon also indicates MFA status:

- Unlocked - MFA is not set up
- Locked - MFA is set up

- Click **Update Multi Factor Authentication**.



- The following instructions will display:



To set up two factor authentication using an authenticator app please go through the following steps:

1. Download a two-factor authenticator app like Microsoft Authenticator for **Windows Phone**, **Android** and **iOS** or Google Authenticator for **Android** and **iOS**.
2. Scan the QR Code or enter this key Unique key into your two factor authenticator app. Spaces and casing do not matter.

QR CODE

3. Once you have scanned the QR code or input the key above, your two factor authentication app will provide you with a unique code. Enter the code in the confirmation box below.

Authenticator Code

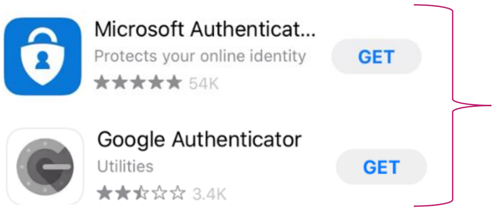
Please Enter Your Authenticator Code

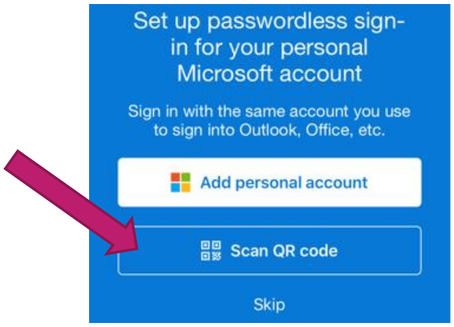
Do not share the QR code or unique key shared on this screen. This information is unique to your account setup and sharing is a HIPPA violation.

Follow these instructions:

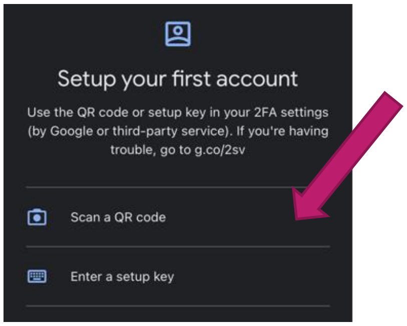
Step 1:
On your mobile device:

- Use the App Store or Google Play Store to download a multifactor authenticator app such as:
  - Microsoft Authenticator, Android and iOS
  - Google Authenticator, Android and iOS
- Open the app after downloading, and the following home screen will display:
- Press **Scan QR Code**.




Set up passwordless sign-in for your personal Microsoft account

Sign in with the same account you use to sign into Outlook, Office, etc.


Setup your first account

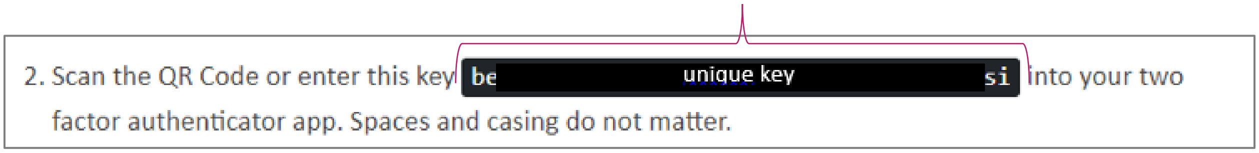
Use the QR code or setup key in your 2FA settings (by Google or third-party service). If you're having trouble, go to g.co/2sv

Step 2:
On your mobile device:

- **Scan the QR Code** on your screen using your camera.

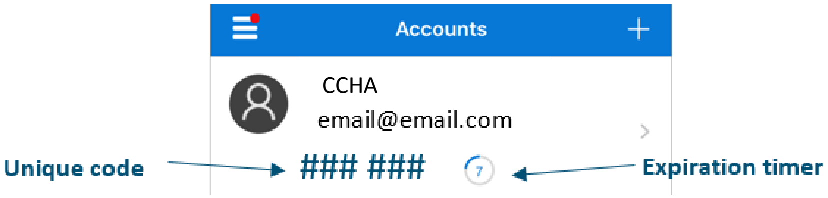
Or

- **Enter unique key** provided in Step 2 into the two factor authentication app by selecting **enter code manually**.


2. Scan the QR Code or enter this key be [redacted] unique key si into your two factor authenticator app. Spaces and casing do not matter.

Step 3:
On your mobile device or your PC:

- The multifactor authentication app will display a unique code.
  - The code will expire and generate a new code.

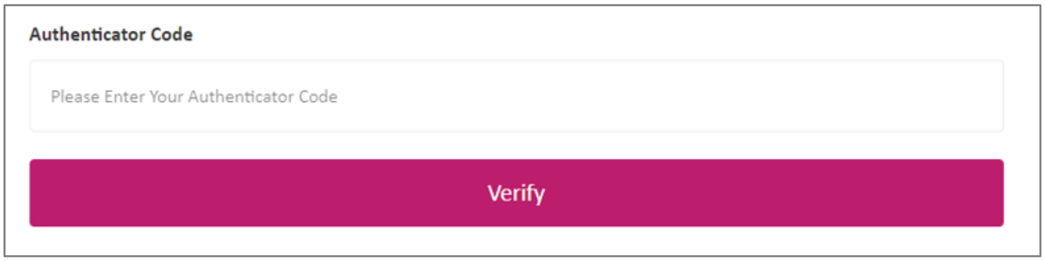


Unique code

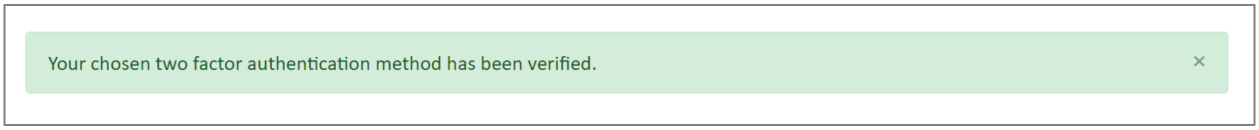
Expiration timer

Step 4:
On your PC:

- Enter the code into the box provided on your mobile device in the *Authenticator Code* box provided on your PC.

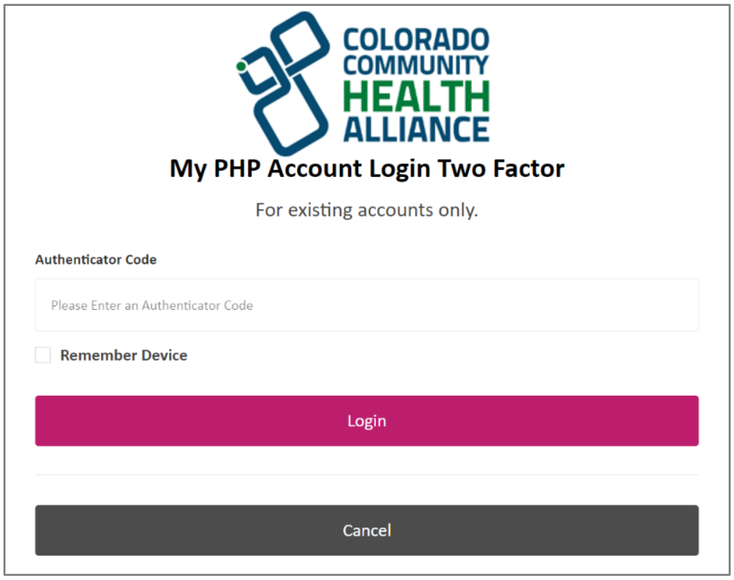


- The following message will display on your *Profile* screen.


Your chosen two factor authentication method has been verified.

- For MFA changes to take effect, you will need to log out and back in.
- Upon login, you will be asked to verify the MFA you set up in the previous steps.

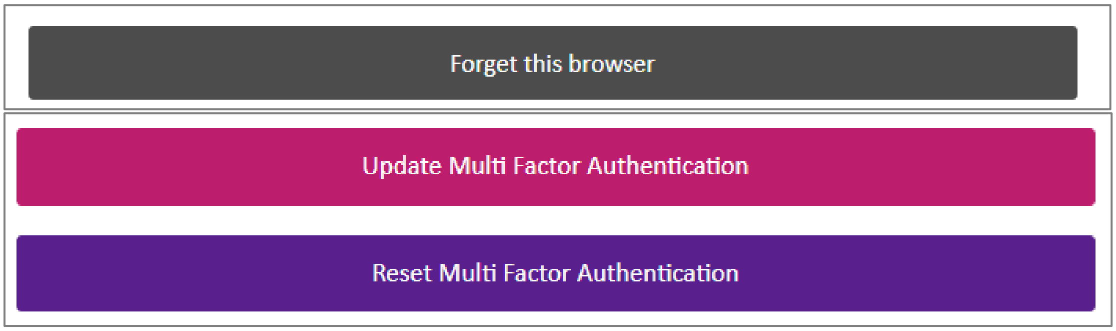
- Enter **Unique Code *from mobile device app*** into the *Authenticator Code* box on your PC.
  - Repeat Steps 3 and 4 above to confirm MFA account.
- Check the box for **Remember Device**.
- Click **Login**.



My PHP Account Login Two Factor

For existing accounts only.

Multifactor Authentication Menu

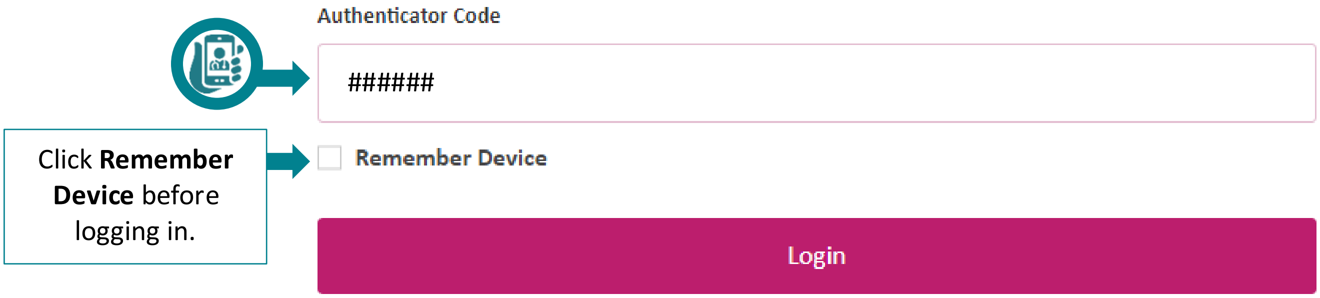

Forget this browser
Update Multi Factor Authentication
Reset Multi Factor Authentication

Once MFA has been successfully set up, your Multifactor menu options will change. Here you can:

- **Forget this browser** – Using the 6-digit code from your authentication app, you can forget and reset your browser security.
- **Update Multi Factor Authentication** – You will be given a new setup screen (QR code and unique key) and can update the multifactor authentication setting using the information provided within your browser and the authentication app on your phone.
    - You can use this option if you did not create an authentication account and need to re-confirm your browser.
- **Reset Multi Factor Authentication** – You will be given a new setup screen (QR code and unique key) and can update the multifactor authentication setting using the information provided within your browser and the authentication app on your phone.

Confirming Browser

After logging out and back in to the Provider Portal, or in instances of a browser reset (e.g., clearing browser cache), you may get a prompt to confirm your browser by entering a new authenticator code from your authentication app. To avoid this in the future, enter your authenticator code and then be sure to click the option to **Remember Device**.

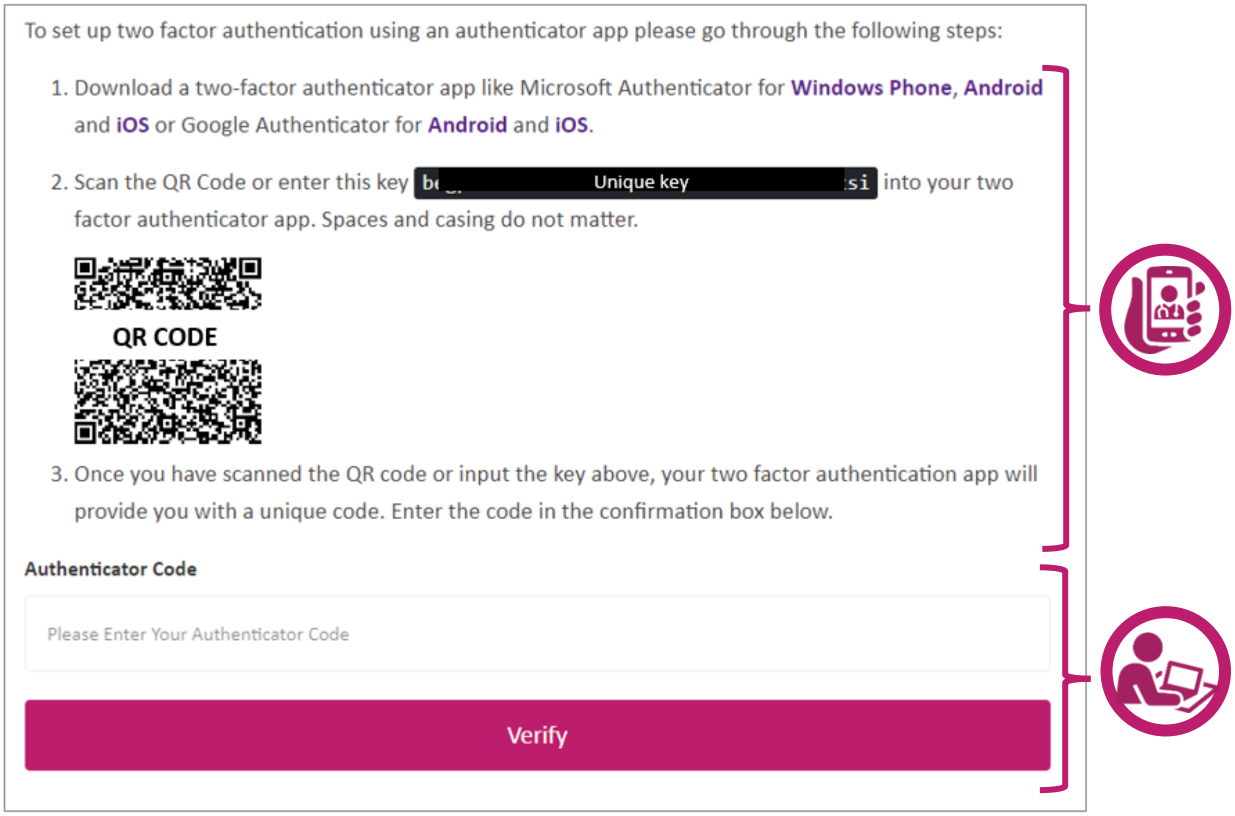

Authenticator Code

######

Click **Remember Device** before logging in.

Setting up Multifactor Authentication AFTER October 26, 2022

- Log into the CCHA Provider Portal, CCHAproviders.com.
- You will see an error message. There will be a link to set up multifactor authentication at the bottom of the webpage. Click on this link
- The following screen will display:



To set up two factor authentication using an authenticator app please go through the following steps:

1. Download a two-factor authenticator app like Microsoft Authenticator for **Windows Phone**, **Android** and **iOS** or Google Authenticator for **Android** and **iOS**.
2. Scan the QR Code or enter this key [redacted] into your two factor authenticator app. Spaces and casing do not matter.
3. Once you have scanned the QR code or input the key above, your two factor authentication app will provide you with a unique code. Enter the code in the confirmation box below.

Authenticator Code

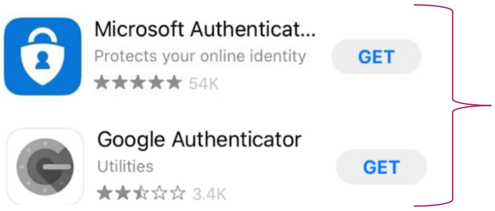
Please Enter Your Authenticator Code

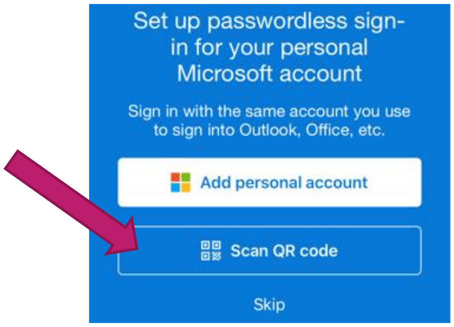
Do not share the QR code or unique key shared on this screen. This information is unique to your account setup and sharing is a HIPPA violation.

Follow these instructions:

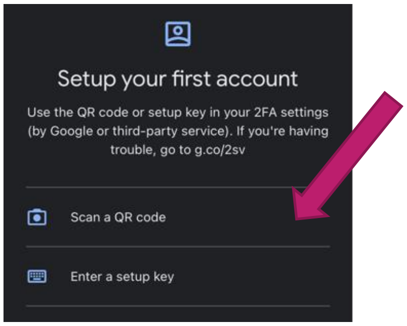
Step 1:
On your mobile device:

- Use the App Store or Google Play Store to download a multifactor authenticator app such as:
    - Microsoft Authenticator, Android and iOS
    - Google Authenticator, Android and iOS
- Open the app after downloading, and the following home screen will display:
- Press **Scan QR Code**.




Set up passwordless sign-in for your personal Microsoft account

Sign in with the same account you use to sign into Outlook, Office, etc.


Setup your first account

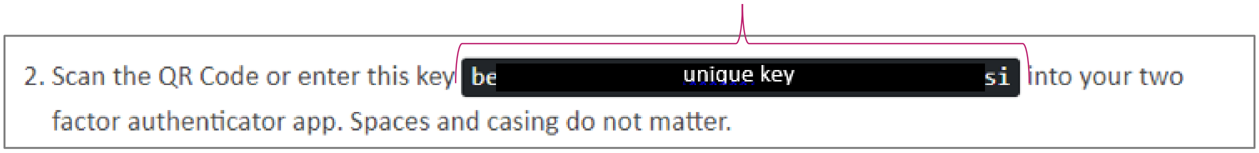
Use the QR code or setup key in your 2FA settings (by Google or third-party service). If you're having trouble, go to g.co/2sv

Step 2:
On your mobile device:

- **Scan the QR Code** on your screen using your camera.

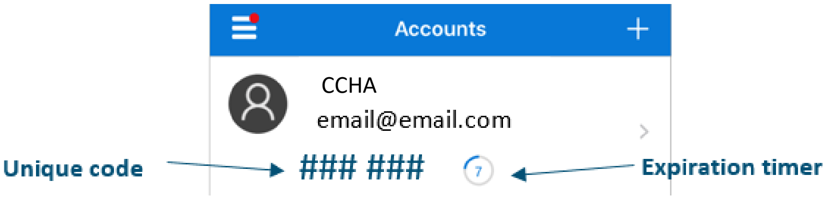
Or

- **Enter unique key** provided in Step 2 into the two factor authentication app by selecting **enter code manually**.


2. Scan the QR Code or enter this key [redacted] into your two factor authenticator app. Spaces and casing do not matter.

Step 3:
On your mobile device or your PC:

- The multifactor authentication app will display a unique code.
    - The code will expire and generate a new code.

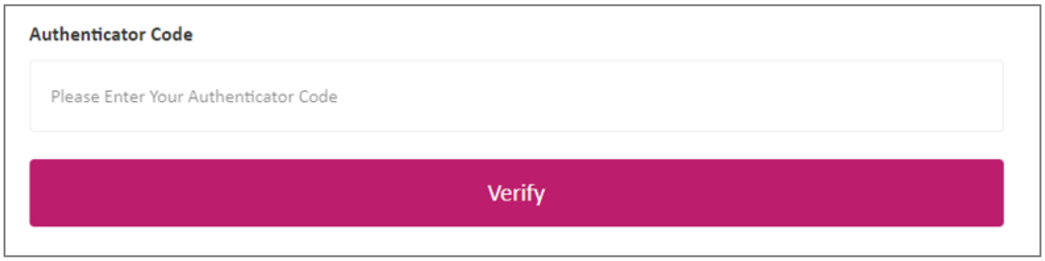

Accounts

CCHA
email@email.com

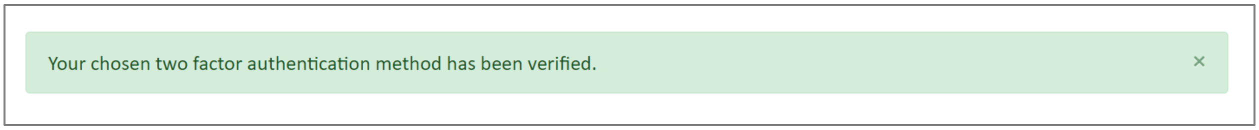
###

Step 4:
On your PC:

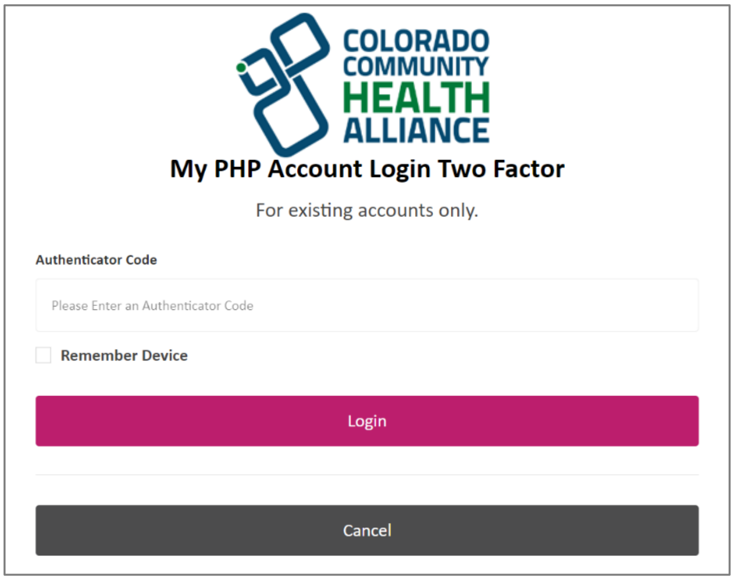
- Enter the code into the box provided on your mobile device in the *Authenticator Code* box provided on your PC.



- The following message will display on your *Profile* screen.


Your chosen two factor authentication method has been verified.

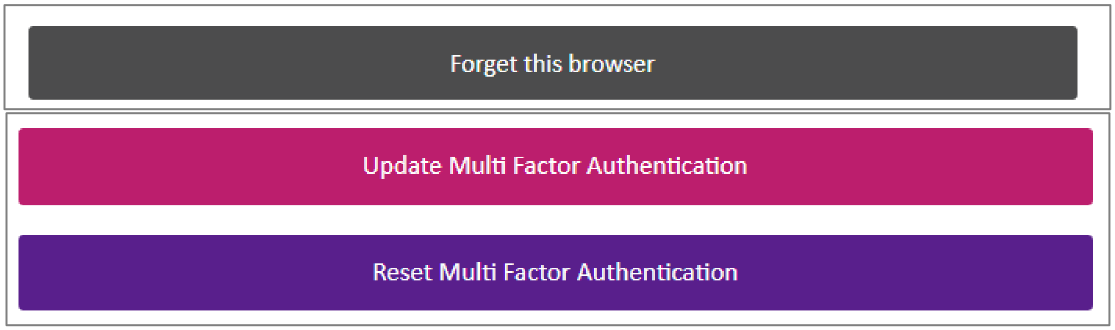
- For MFA changes to take effect, you will need to log out and back in.
- Upon login, you will be asked to verify the MFA you set up in the previous steps.
- Enter **Unique Code *from mobile device app*** into the *Authenticator Code* box on your PC.
  - Repeat Steps 3 and 4 above to confirm MFA account.
- Check the box for **Remember Device**.
- Click **Login**.



My PHP Account Login Two Factor

For existing accounts only.

Multifactor Authentication Menu

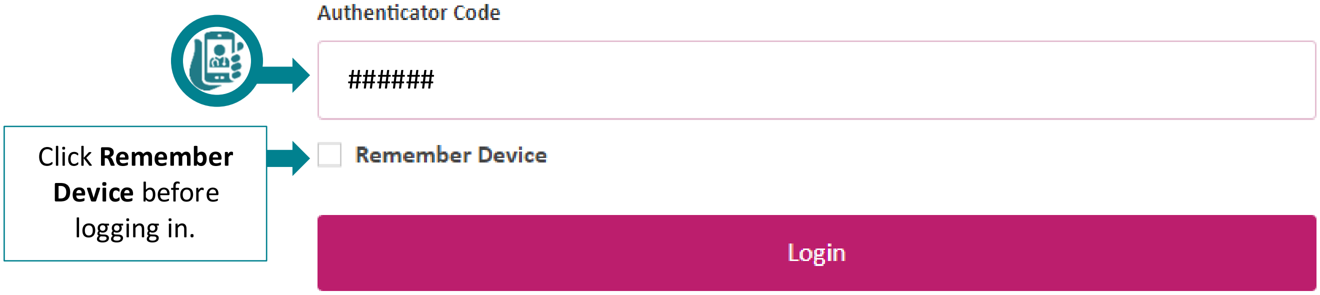

Forget this browser
Update Multi Factor Authentication
Reset Multi Factor Authentication

Once MFA has been successfully set up, your Multifactor menu options will change. Here you can:

- **Forget this browser** – Using the 6-digit code from your authentication app, you can forget and reset your browser security.
- **Update Multi Factor Authentication** – You will be given a new setup screen (QR code and unique key) and can update the multifactor authentication setting using the information provided within your browser and the authentication app on your phone.
    - You can use this option if you did not create an authentication account and need to re-confirm your browser.
- **Reset Multi Factor Authentication** – You will be given a new setup screen (QR code and unique key) and can update the multifactor authentication setting using the information provided within your browser and the authentication app on your phone.

Confirming Browser

After logging out and back in to the Provider Portal, or in instances of a browser reset (e.g., clearing browser cache), you may get a prompt to confirm your browser by entering a new authenticator code from your authentication app. To avoid this in the future, enter your authenticator code and then be sure to click the option to **Remember Device**.



Click **Remember Device** before logging in.