Provider Portal – Two-Factor Authentication

Logging in with a username and password is vulnerable to phishing and other methods by which malicious or unauthorized users can gain access to your web applications. To implement an extra layer of security, Michigan Medicine has implemented two-factor authentication, which requires community users to enter their standard username and password plus a randomly generated one-time passcode to log in. This document covers the steps to set up two-factor authentication.

There are two methods for setting up two-factor authentication:

1. **Mobile application** on your smartphone, or
2. **Email**

For step-by-step instructions on your preferred method of authentication, go to the page listed below:

Setting up Two-Factor Authentication by Mobile App ..... pg. 2

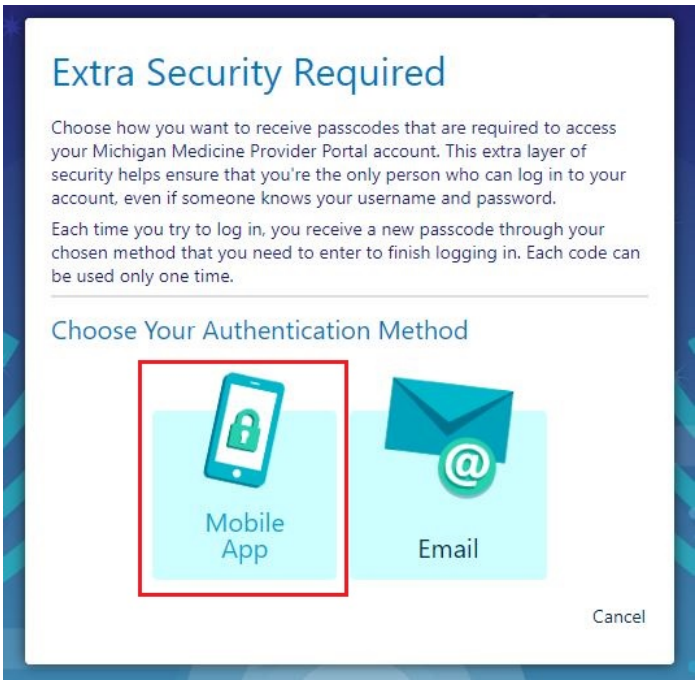
Setting up Two-Factor Authentication by Email ..... pg. 5

Authentication Tips ..... pg. 8

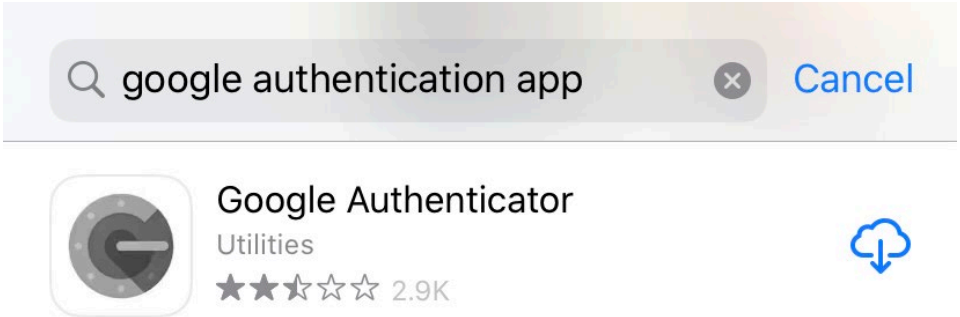
Setting up Two-Factor Authentication – Mobile Application Method

1. Go to the Provider Portal log-in page (https://www.providerportal.uofmhealth.org/) and log in using your Provider Portal username and password.

2. Click on the "**Mobile App**" icon

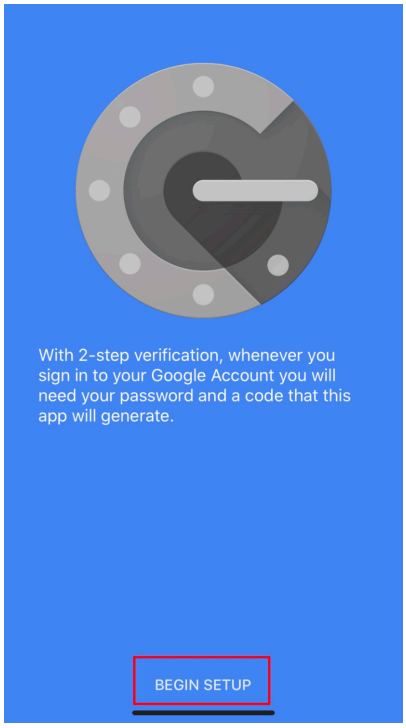


3. Go to your smart phone app store and download an authenticator app. Popular authentication apps include *Google Authenticator*, *Authy*, and *Epic Authenticator*. For this tip sheet process, we will be using **Google Authenticator**:

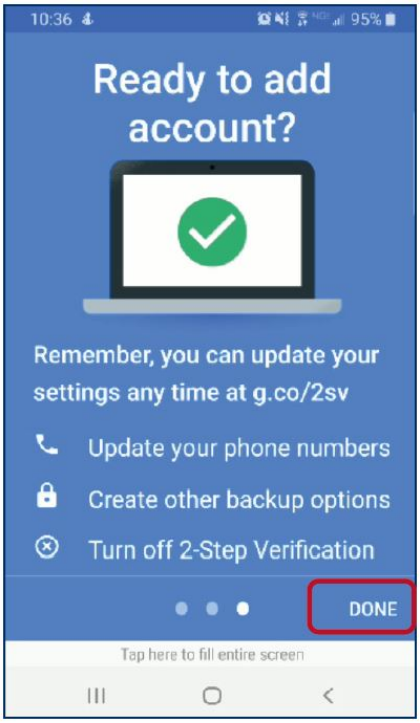


4. Open the Google Authenticator app, and click "**Begin Setup**" (iPhone) or "**Done**" (Android).

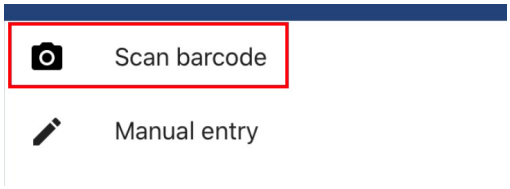
iPhone:



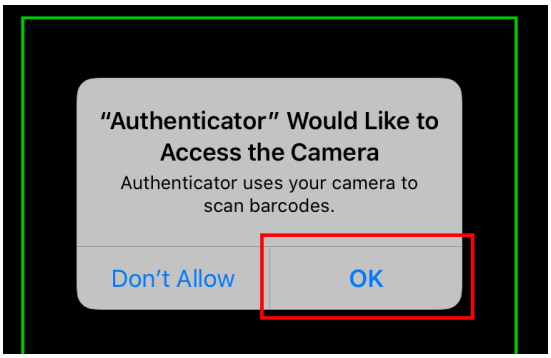
Android:

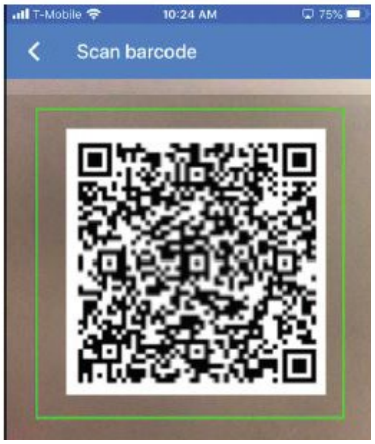


5. Click "**Scan barcode**"

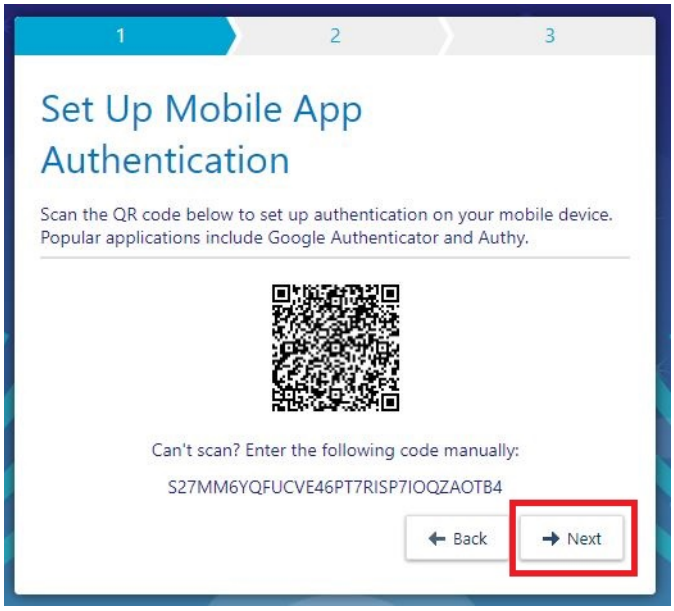


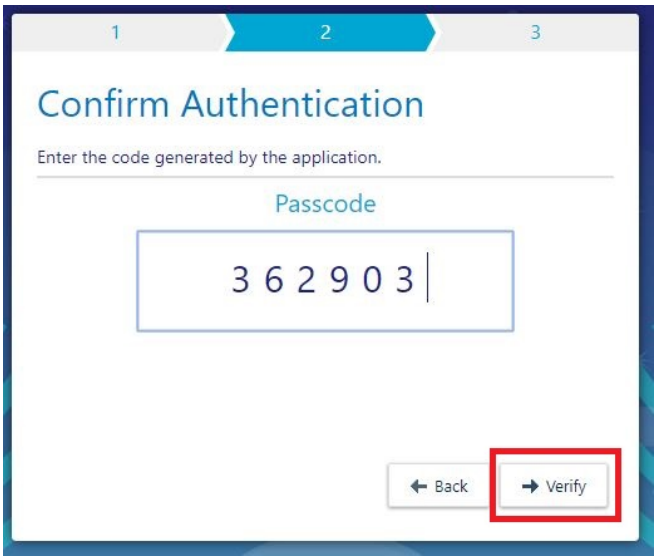
6. Allow access to the camera on your phone (iPhone) and then aim your smartphone camera at the barcode on your computer screen.



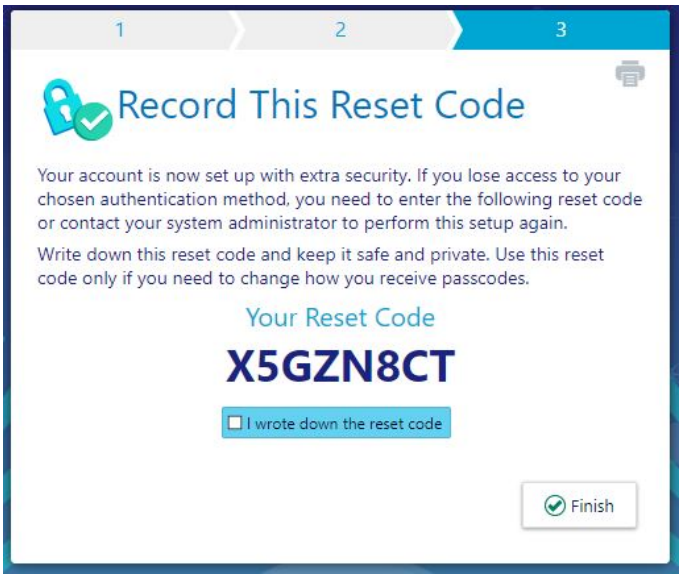


7. Once the barcode has scanned and you see the verification code on your smart phone, click "**Next**" on your computer screen. On the next screen enter the code from your smart phone.





8. Write down the Reset Code given on the next screen and click the "**I wrote down the reset code**" check box. This will be needed if you ever want to change how you set up two-factor authentication.



9. Click "**Finish**" and you will be logged into the Provider Portal.

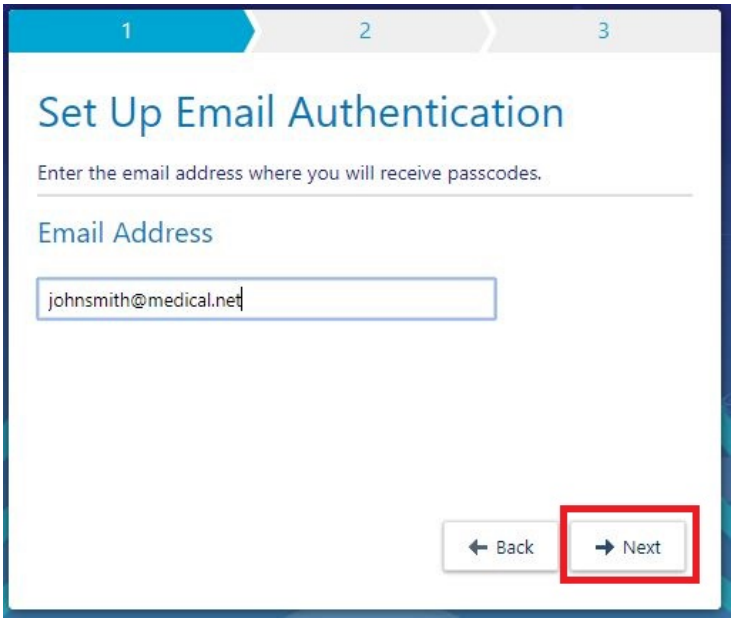
***NOTE**: The next time you log in to the Provider Portal, you will not have to scan the barcode. You can just open the Google Authenticator app on your phone and enter the new code when prompted.*

Setting up Two-Factor Authentication – Email Method

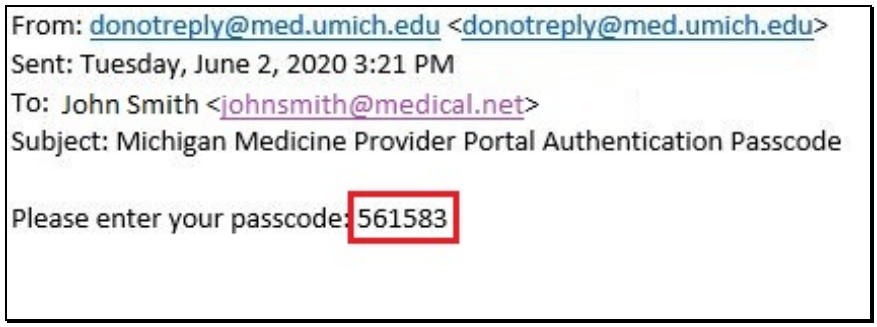
1. Go to the Provider Portal log-in page (https://www.providerportal.uofmhealth.org/) and log in using your Provider Portal username and password.

2. Click on the **Email** icon.

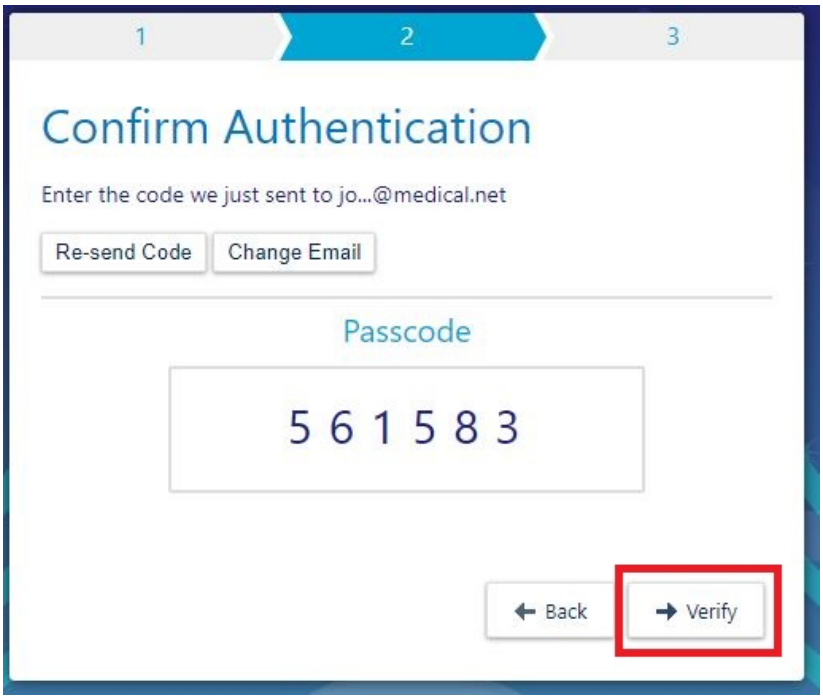
3. Enter your email address, click "**Next**".



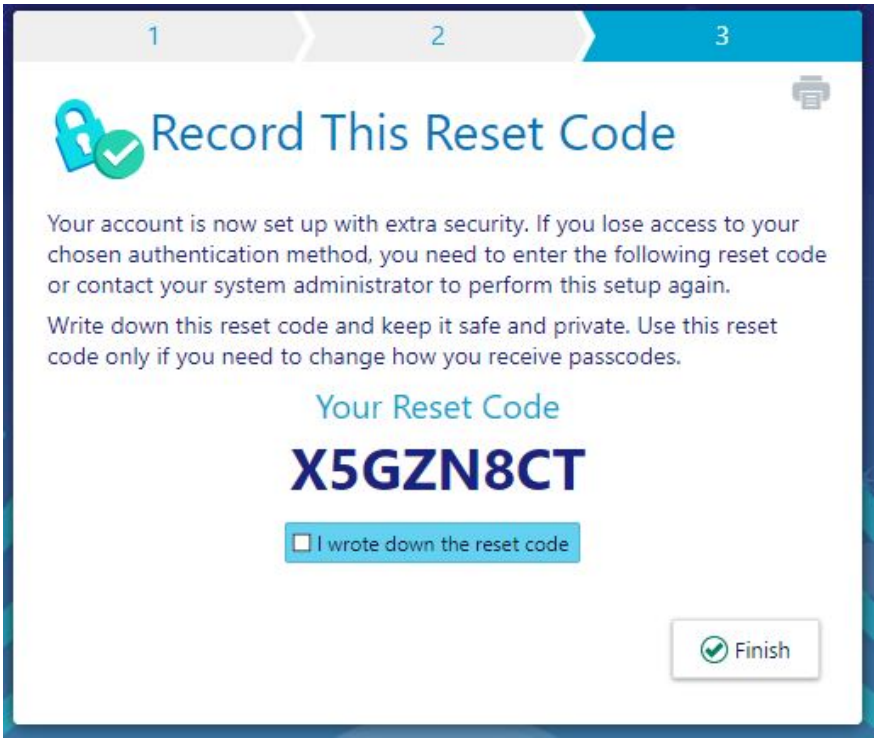
4. Go to your email inbox and open the passcode email. The subject of the email with be: "***Michigan Medicine Provider Portal Authentication Passcode***".



5. Enter the passcode from the email into the passcode box, then click "**Verify**"
   - *Note: Copy & Pasting the passcode from the email into the box is quicker and ensures no mistakes*



6. Write down the Reset Code given on the next screen and click the "**I wrote down the reset code**" check box. This will be needed if you ever want to change how you set up two-factor authentication.



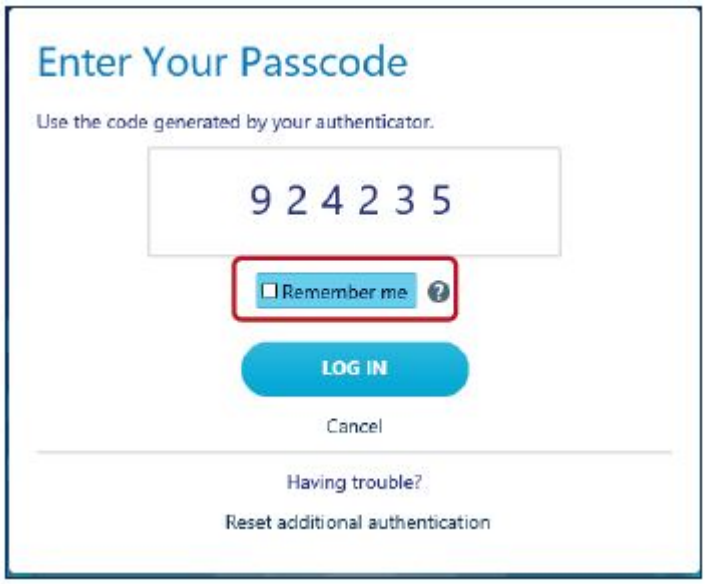
7. Click "**Finish**" and you will be logged into the Provider Portal.

***NOTE**: The next time you log in to the Provider Portal, the authentication code will be sent to the email address you specified during set up.*

Authentication Tips

Now that you've set up two-factor authentication to access the Provider Portal, you will be prompted for an authentication code each time you access the Provider Portal.

If you access the Provider Portal multiple times each day, use the ***Remember Me*** setting to streamline the process. To enable the Remember Me setting, click the checkbox under the area you enter your passcode. This will allow you to bypass the two-factor authentication process for the remainder of the day.



NOTE: Two-factor authentication will be bypassed ONLY when the following conditions are met:

- Cookies are enabled on the workstation.
- The same user is logging in at the same workstation.
    - If another user logs in to the same workstation, "*Remember Me*" is reset.
- If the user logs on to another workstation, "*Remember Me*" is reset.

Portal Help Desk Assistance

If you are no longer able to receive log in codes via the authentication method you selected, or are having issues with resetting your two-factor authentication, please contact the Portal Help Desk at **734-615-0872.**