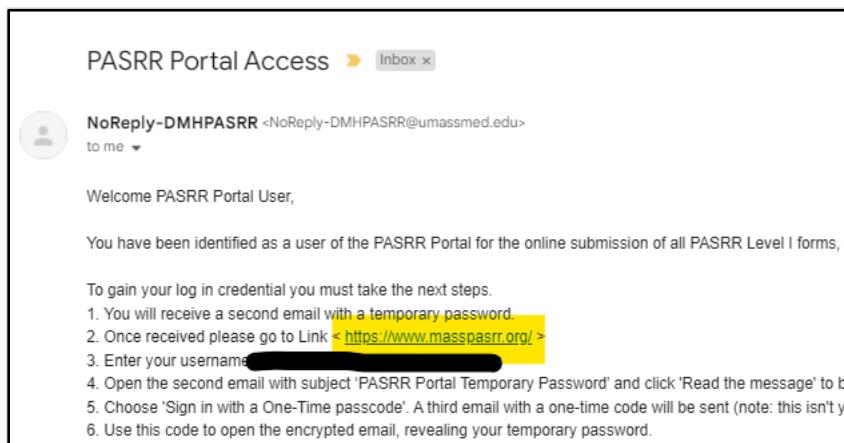


PASRR Initial Login Guide

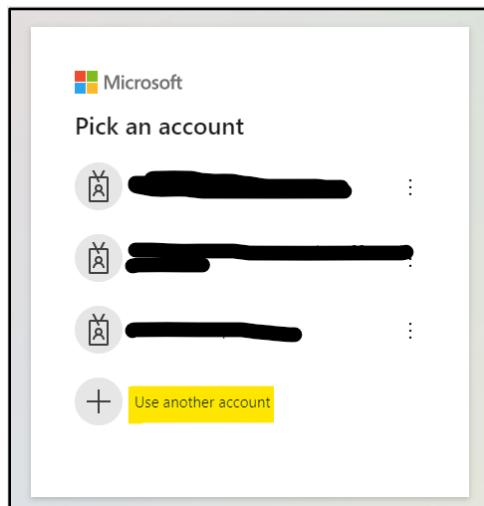
Access to the Preadmission Screening and Resident Review (PASRR) portal is a multistep process, the first of which consists of a Learning Management System (LMS) training component. Once training is complete, you will receive a series of emails consisting of an access email with instructions on how to gain access to the portal and set up your account. Please follow the steps below using google chrome incognito mode to set up your account the first time you log in.

Step 1. You will receive an email with the subject line “PASRR Portal Access” from [No-Reply-DMHPASRR@umassmed.edu](mailto>No-Reply-DMHPASRR@umassmed.edu). Please note that this email may be in your junk mail or spam folder. If you did not receive the email OR need a new email sent, please contact DMHPASRR@umassmed.edu with the subject line “New PASRR Portal Access email needed”.

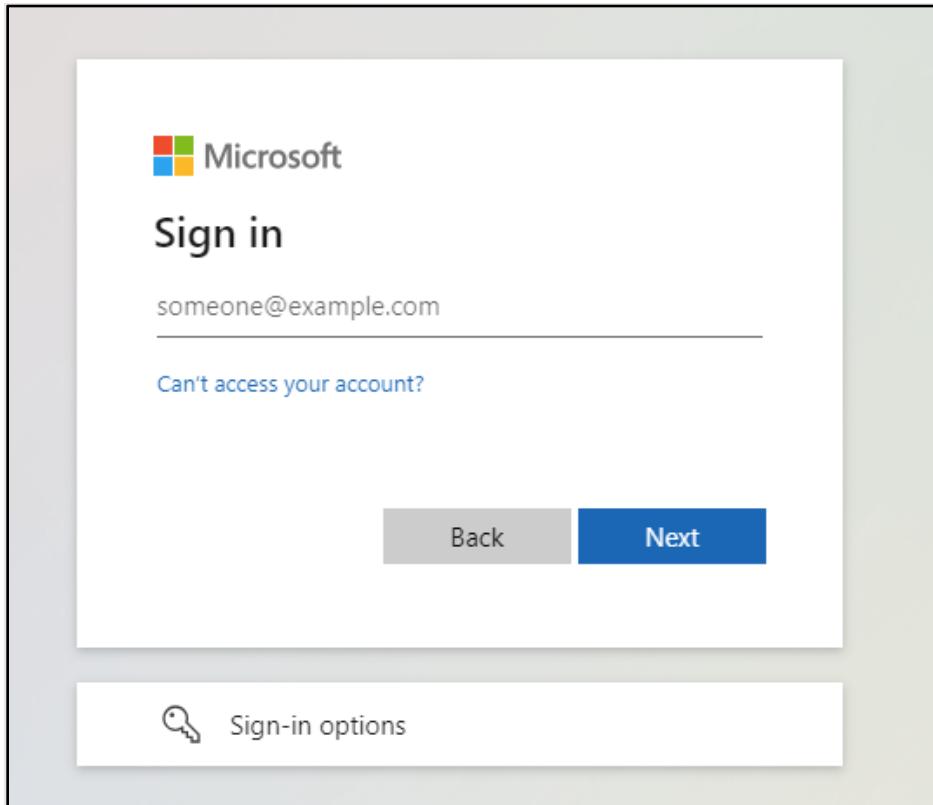
Step 2. Within that email, click on the link highlighted below.



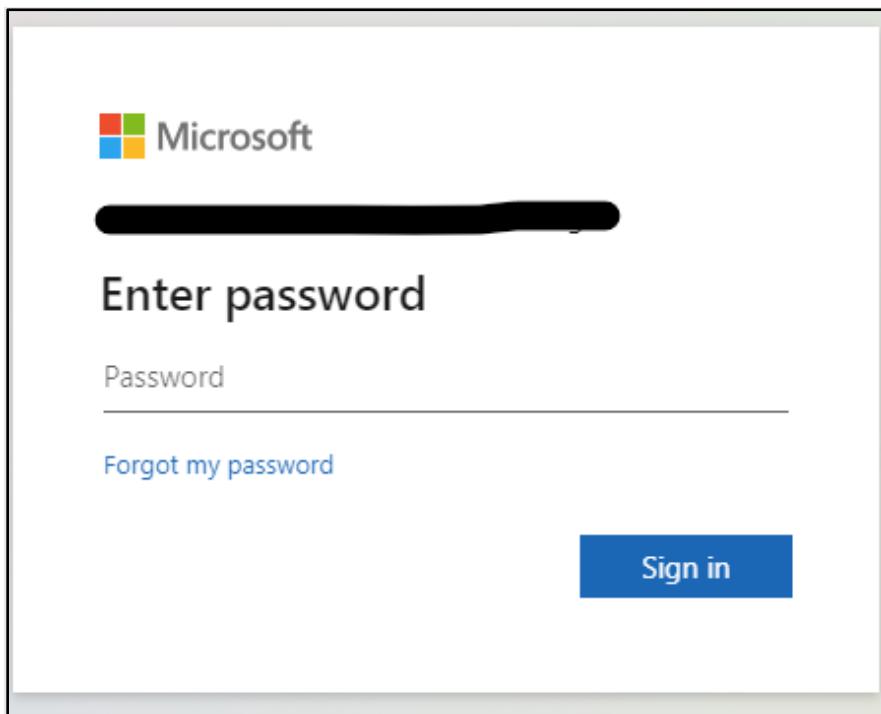
Step 3. Your web browser will be redirected to a Microsoft login page. Choose the “Use another account” option on the bottom of the Microsoft “Pick an account” screen.



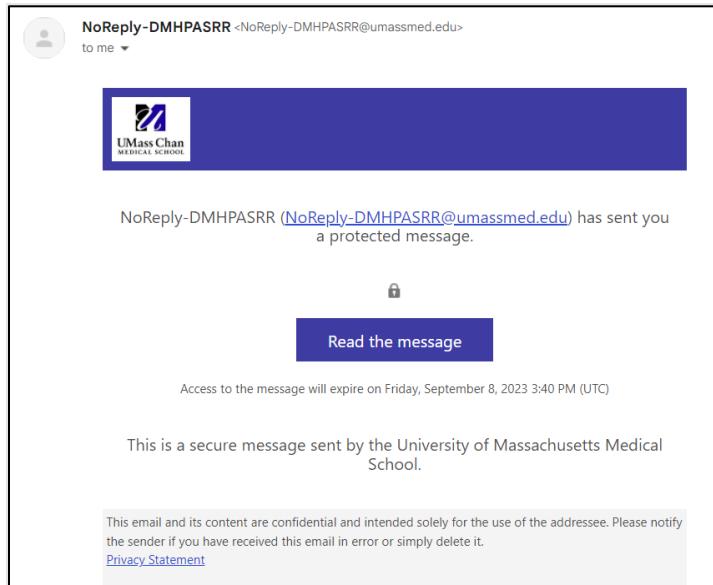
Step 4. Copy the username from the PASRR portal Access email described in Step 2 and enter it in the “Sign in” screen. Click “Next”.



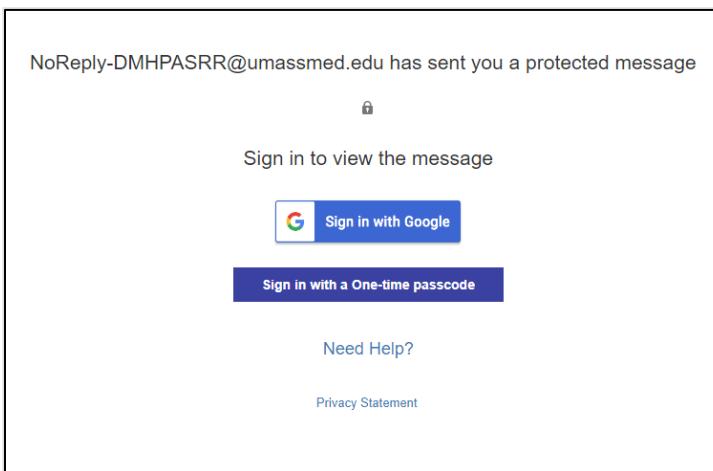
Step 5. The “Enter password” screen will appear. [STOP on this screen](#). Do not enter anything here for now.



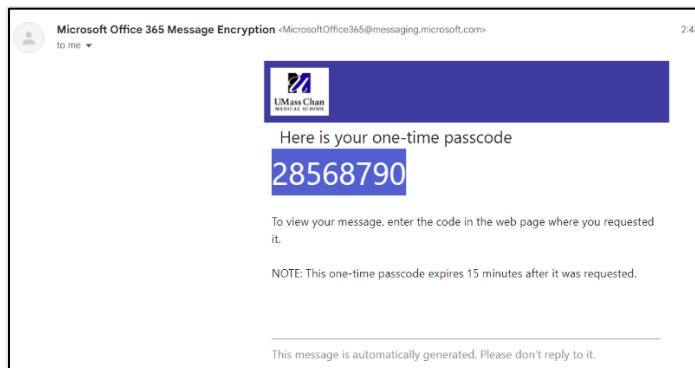
Step 6. Locate the email with the subject line “Secure- PASRR Portal Temporary Password”. Click on “Read the message”.



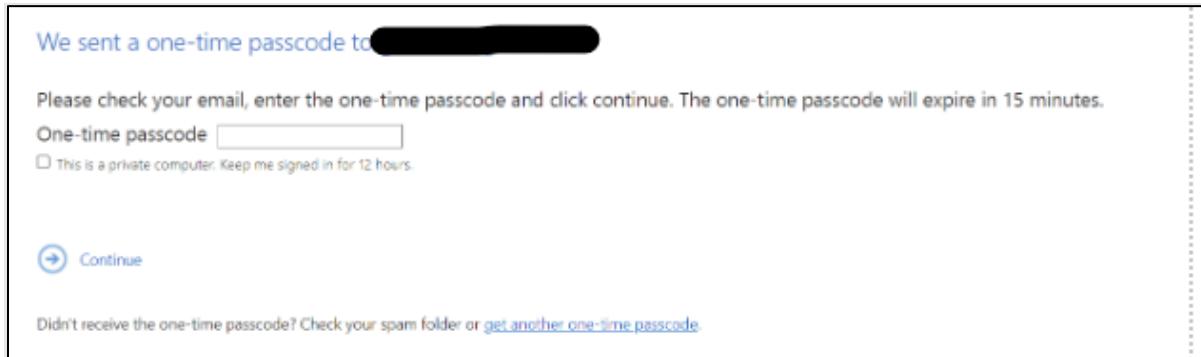
Step 7. A new window will open. Click on “Sign in with a One-time passcode” option.



Step 8. You will receive an email with the subject line “Your one-time passcode to view the message”. This email contains a one-time passcode.



Step 9. Enter the one-time passcode from this email and click “Continue”.

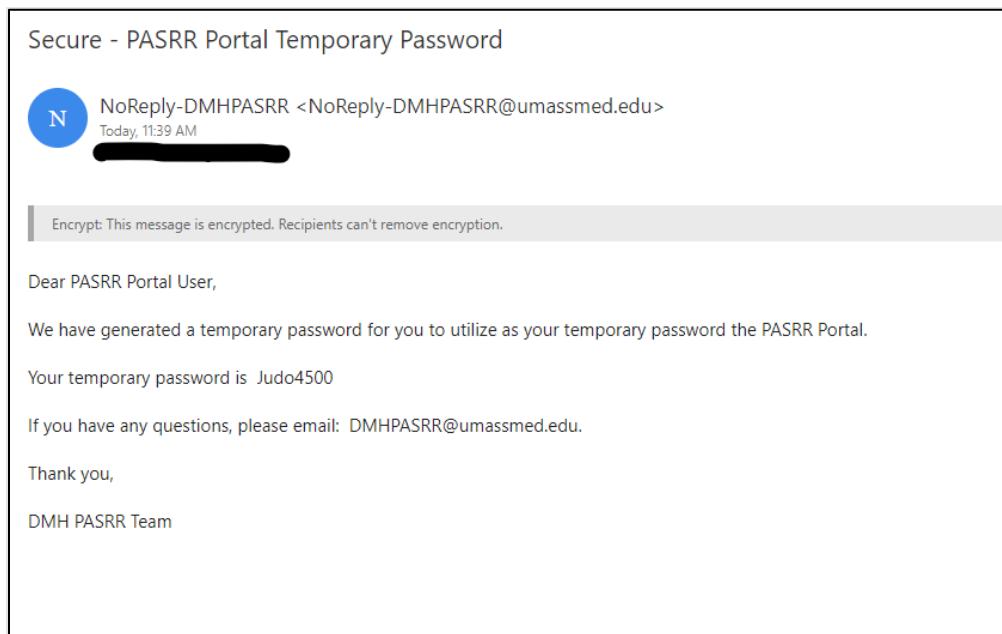


We sent a one-time passcode to [REDACTED]
Please check your email, enter the one-time passcode and click continue. The one-time passcode will expire in 15 minutes.
One-time passcode [REDACTED]
 This is a private computer. Keep me signed in for 12 hours.

 Continue

Didn't receive the one-time passcode? Check your spam folder or [get another one-time passcode](#).

Step 10. The temporary password will be displayed in your web browser.



Secure - PASRR Portal Temporary Password

NoReply-DMHPASRR <NoReply-DMHPASRR@umassmed.edu>
Today, 11:39 AM
[REDACTED]

Encrypt: This message is encrypted. Recipients can't remove encryption.

Dear PASRR Portal User,

We have generated a temporary password for you to utilize as your temporary password the PASRR Portal.

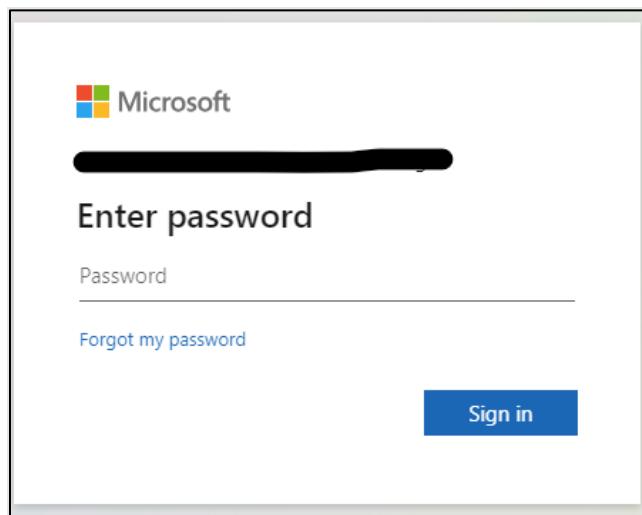
Your temporary password is Judo4500

If you have any questions, please email: DMHPASRR@umassmed.edu.

Thank you,

DMH PASRR Team

Step 11. Return to the “Enter password” screen. Enter your temporary password.



Microsoft

[REDACTED]

Enter password

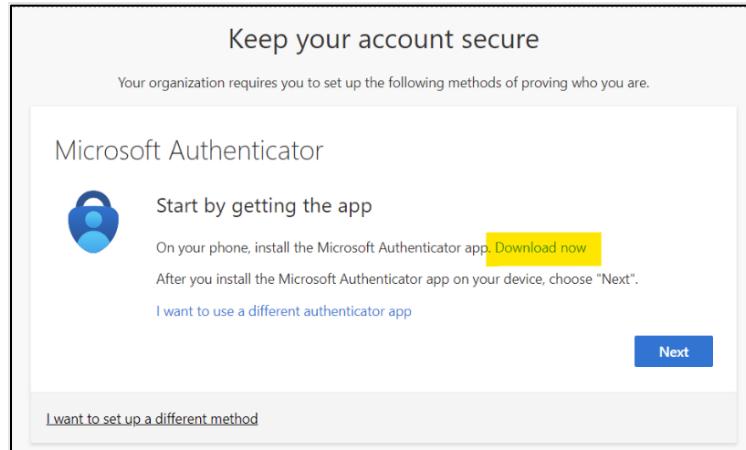
Password

[Forgot my password](#)

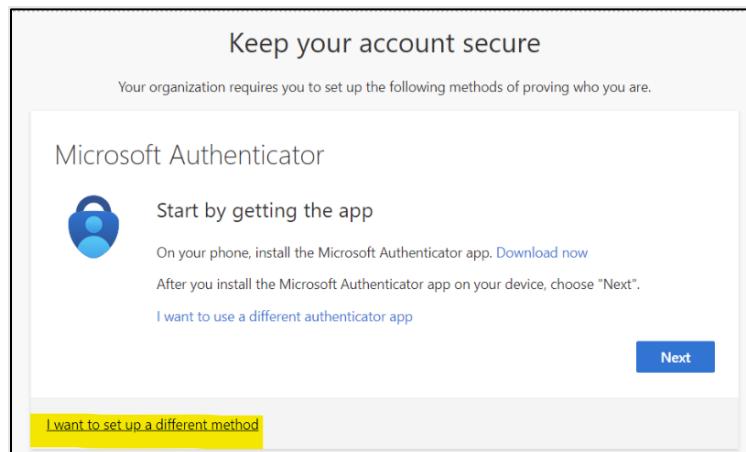
Sign in

Step 12. You will be prompted to select how you would like to authenticate your account each time you log into the portal. You have two options:

Option 1: Download the Microsoft Authenticator application on phone by clicking “Download now” link.

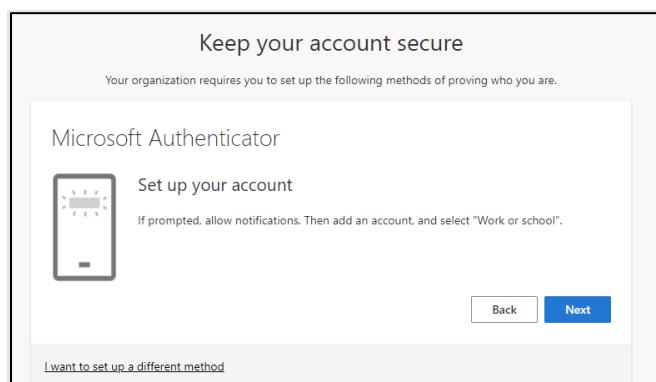


Option 2: Click on the “I want to set up a different method”. If you select this option, skip to Step 18 on page 7 of this uder guide.

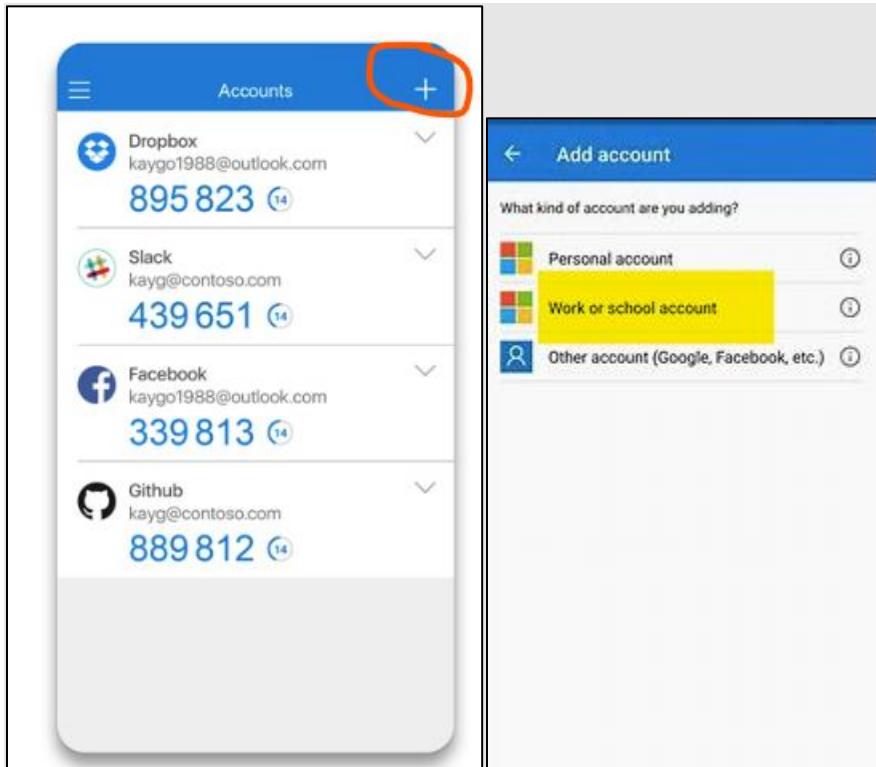


Step 13. Only for Option 1. Download the Microsoft Authenticator application on your phone.

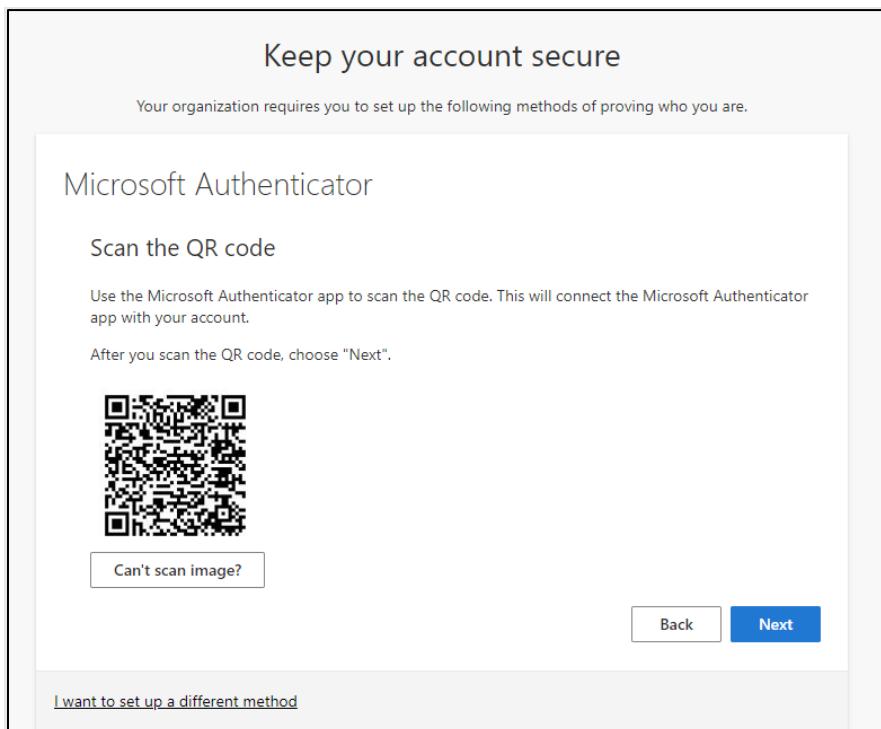
Step 14. Only for Option 1. Click “Next”.



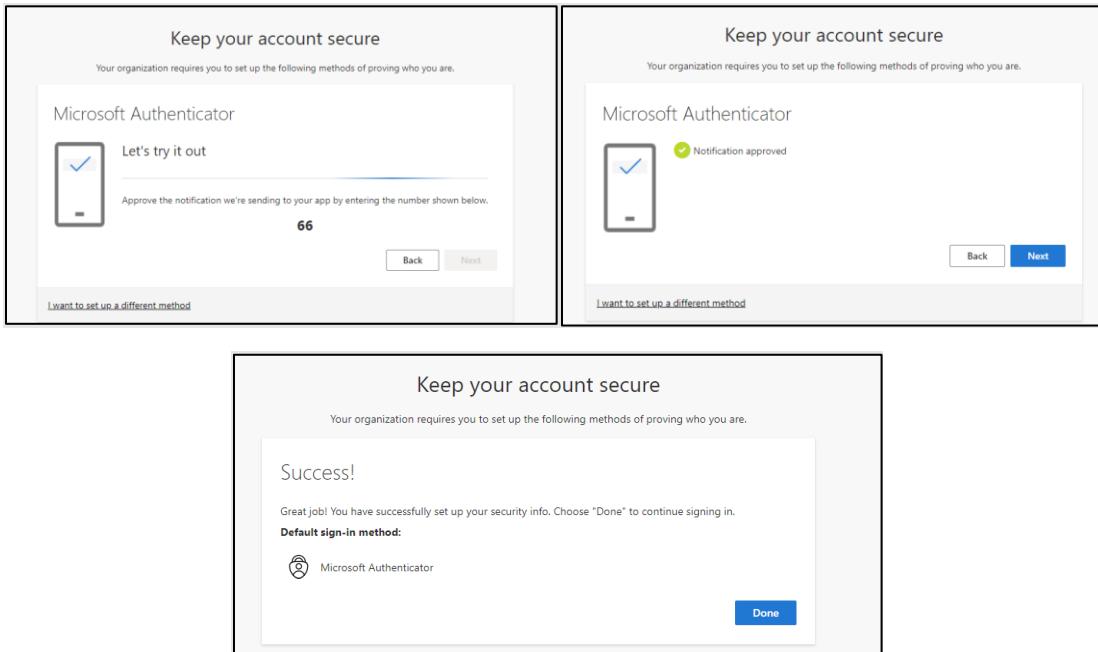
Step 15. Only for Option 1. Open the Microsoft Authenticator application on your phone and click on the “+” symbol. Select “Work or School account”.



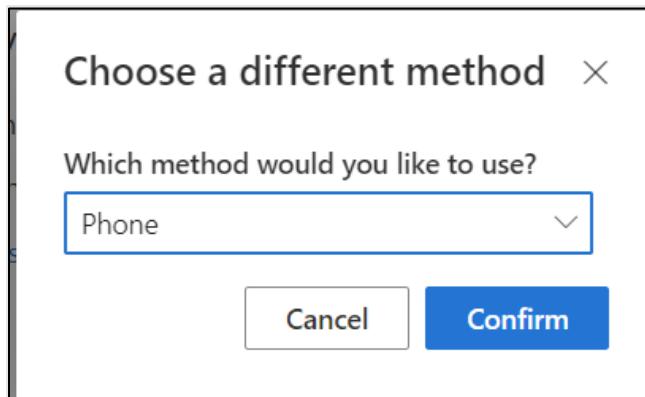
Step 16. Only for Option 1. Select Scan QR code on phone and scan the code from the browser. Click “Next”.



Step 17. Only for Option 1. Enter the 2-digit number on phone. Click “Next”, “Next”, and “Done”. Skip to Step 22 on page 10 of this user guide.



Step 18. Only for Option 2. If you selected Option 2 at Step 12, select “Phone” from the drop down menu. Click “Confirm”.



IMPORTANT: If selecting this option, you will need to have access to this phone number each time you login to the PASRR Portal.

Step 19. Only for Option 2. Enter phone number and select how you would like to authenticate, through text message or through phone call, each time you access the PASRR Portal.

Select “Text me a code” if you would like to authenticate via text each time you access the PASRR Portal. Click “Next”.

Select “Call me” if you would like to authenticate via phone call each time you access the PASRR Portal. Click “Next”.

Keep your account secure

Your organization requires you to set up the following methods of proving who you are.

Phone

You can prove who you are by answering a call on your phone or texting a code to your phone.

What phone number would you like to use?

Text me a code
 Call me

Message and data rates may apply. Choosing Next means that you agree to the [Terms of service](#) and [Privacy and cookies statement](#).

[I want to set up a different method](#)

Keep your account secure

Your organization requires you to set up the following methods of proving who you are.

Phone

We just sent a 6 digit code to +1 7179407256. Enter the code below.

[Resend code](#)

[I want to set up a different method](#)

Keep your account secure

Your organization requires you to set up the following methods of proving who you are.

Phone

You can prove who you are by answering a call on your phone or texting a code to your phone.

What phone number would you like to use?

Text me a code
 Call me

Message and data rates may apply. Choosing Next means that you agree to the [Terms of service](#) and [Privacy and cookies statement](#).

[I want to set up a different method](#)

Step 20. Only for Option 2. Answer the phone call and press the “#” key. The screen below will be displayed. Click “Next”.

Keep your account secure

Your organization requires you to set up the following methods of proving who you are.

Phone

 Call answered. Your phone was registered successfully.

Next

Step 21. Only for Option 2. Success message will be displayed. Click “Done”.

Keep your account secure

Your organization requires you to set up the following methods of proving who you are.

Success!

Great job! You have successfully set up your security info. Choose "Done" to continue signing in.

Default sign-in method:

 Phone [REDACTED]

Done

Step 22. For both options. The “Data Access Agreement” will be displayed. Review and click on “I Accept”. Click “Confirm”.



Log Out

Data Access Agreement
Non-ForHealth Consulting at UMass Chan Medical School Users

I acknowledge and agree that the security of the ForHealth Consulting at UMass Chan Medical School (ForHealth) computer systems and the privacy and security of electronic data in those systems is of utmost priority. As a condition of obtaining access to ForHealth systems and/or electronic data, I agree that I will:

1. Agree to use the assigned user account only for its approved purpose.
2. Agree to use the assigned user account only for its intended purpose.
3. Not transmit or post any information utilizing the ForHealth system that is unrelated to or beyond the scope of my permission to utilize the system.
4. Keep confidential all information pertaining to the security of ForHealth systems.
5. Treat as confidential all user IDs and passwords needed to gain access to ForHealth systems or electronic data.
6. Not transmit personally-identifiable or confidential data over open networks unless specifically authorized and unless encrypted.
7. Not attempt to access data which is not necessary to achieve the purpose of my access authorization.
8. Not attempt to discover the password(s) of any other ForHealth system user by any means.
9. Not circumvent or attempt to circumvent any security mechanism or procedure applicable to ForHealth systems or to ForHealth electronic data.
10. Not use ForHealth systems to harass, threaten or stalk any individual.
11. Not install any applications on the ForHealth system.
12. Not attempt to intercept or otherwise monitor any ForHealth computer systems, including logins, email, or any other type of ForHealth network traffic.
13. Not attempt to access individually-identified, client, or personnel records, student grades or financial records, or any other electronic records in the ForHealth Systems reasonably expected to be confidential.
14. Accept responsibility for the preservation, privacy and security of ForHealth data in my possession.
15. Not do anything to deface or alter the identification of their assigned user account while using our system.
16. Not use ForHealth systems to commit any unauthorized or illegal acts.
17. Immediately notify ForHealth verbally (by calling 508-289-6220) and in writing (by emailing PrivacyandCompliance@umassmed.edu), if I become aware of any actual or suspected security breach to ForHealth systems and/or electronic data.
18. Immediately notify ForHealth (by calling 508-289-6220) and in writing (by emailing PrivacyandCompliance@umassmed.edu), if I become aware of any actual or suspected security breach to ForHealth systems and/or electronic data.
19. Immediately notify ForHealth if I receive data not intended for me and arrange for its secure return, re-transmission, or destruction, as ForHealth directs.
20. Comply with all applicable Premission Screening and Resident Review (PASRR) rules and procedures; and
21. Comply with all applicable state and federal laws which govern the use and security of computer systems and data, personal information, personal data, protected health information, and patient identifying information including but not limited to the Federal Copyright Law, the Computer Fraud and Abuse Act of 1986, the Electronic Communications Privacy Act of 1986, the Computer Security Act of 2000, the Health Insurance Portability and Accountability Act of 1996, Massachusetts General Laws Chapter 93H and Chapter 95A, the Health Information Technology for Economics and Clinical Health Act of 2009, and 42 Code of Federal Regulations Part 2.

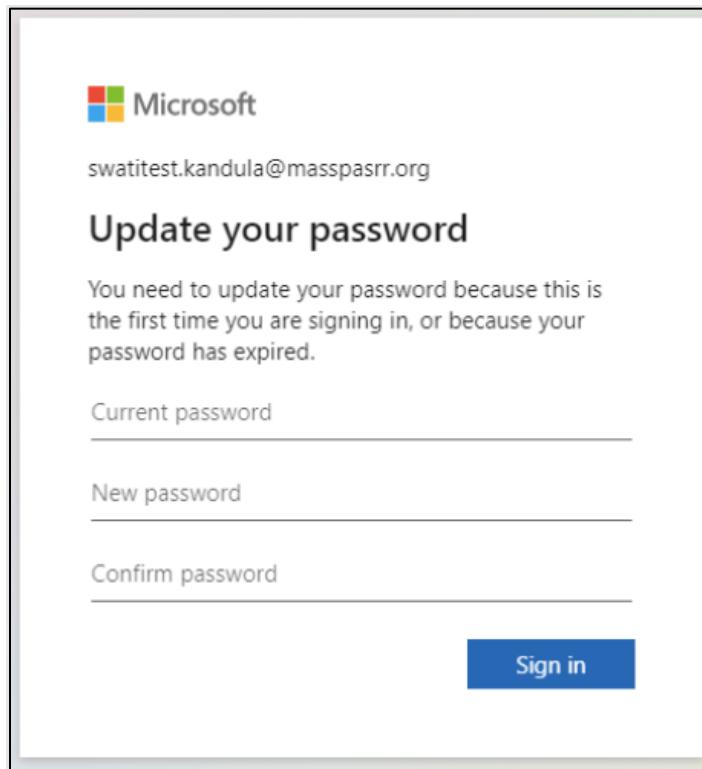
I further acknowledge that the termination or expiration of my access to ForHealth systems and/or electronic data will not relieve me of my obligations under this Agreement to keep confidential the personally identifiable data or ForHealth network security information I may have accessed in connection with this agreement.

Acceptance of Agreement Online is equal to user's agreement to terms.

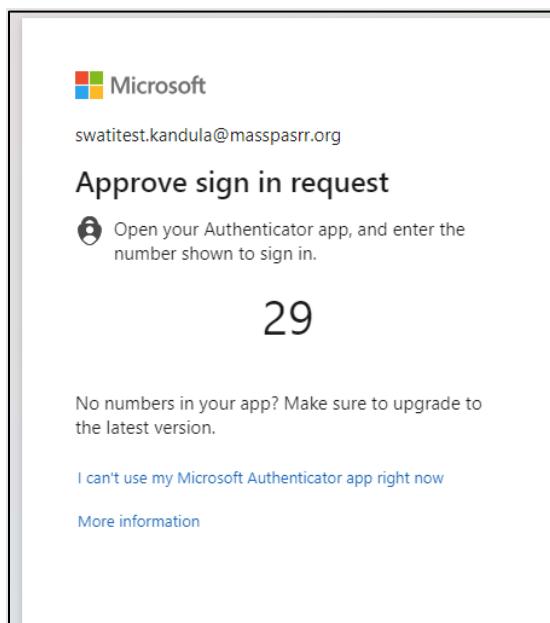
I Accept

Confirm

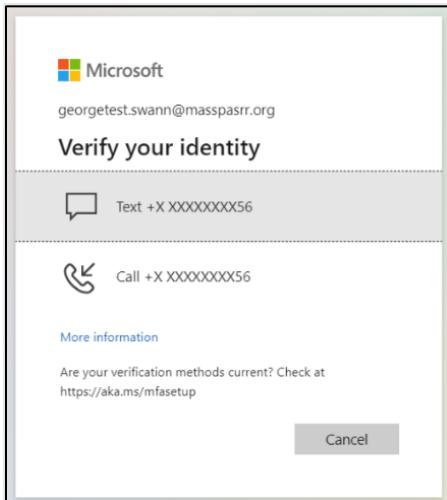
Step 23. For both options. Enter the temporary password from “Secure - PASRR Portal Temporary Password” email into “Current password” field. Then, enter your new password in both New and Confirm Password below. (New password must be 8 digits and must contain a lowercase character, uppercase character, number, and symbols.)



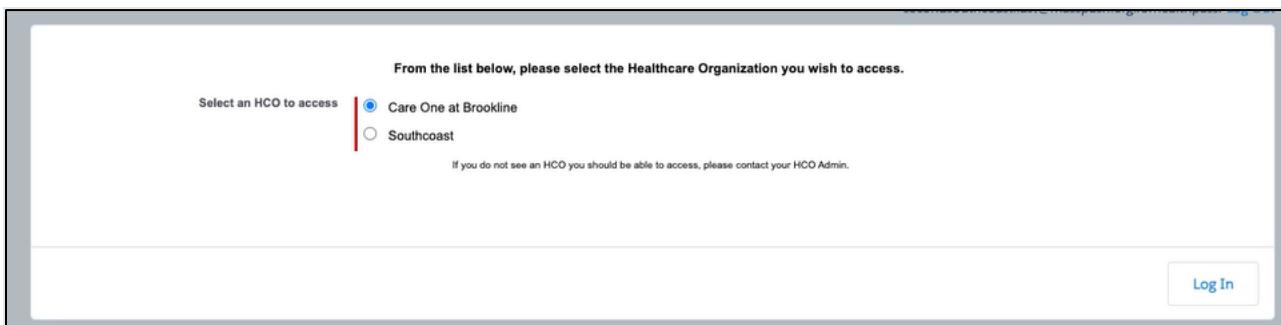
Step 24. Only for Option 1. If you chose to authenticate your account using the Microsoft Authenticator app, enter the 2-digit number from this screen onto the Microsoft Authenticator app on phone.



Step 25. Only for Option 2. Select the call or text option. Press “#” on the call received or enter the code received in text.



Step 26. For both options. Select your Health Care Organization to log in. You will not see this screen if you are registered for only one organization.



Step 24. Congratulations! You have successfully logged into the PASRR Portal.

Next time you access the portal, click on <https://www.masspasrr.org>. Sign in with PASRR username, password, and your opted multifactor authentication

Troubleshooting

If you see the error below, click on <https://www.masspasrr.org>, which will bring you to the password screen. Sign in with your PASRR username, password, and your opted multifactor authentication.



If you see the below error, sign out and select PASRR account (<firstname.lastname@masspasrr.org>), and sign in with your PASRR username, password, and your opted multifactor authentication.

