

How to Reset Multi-Factor Authentication

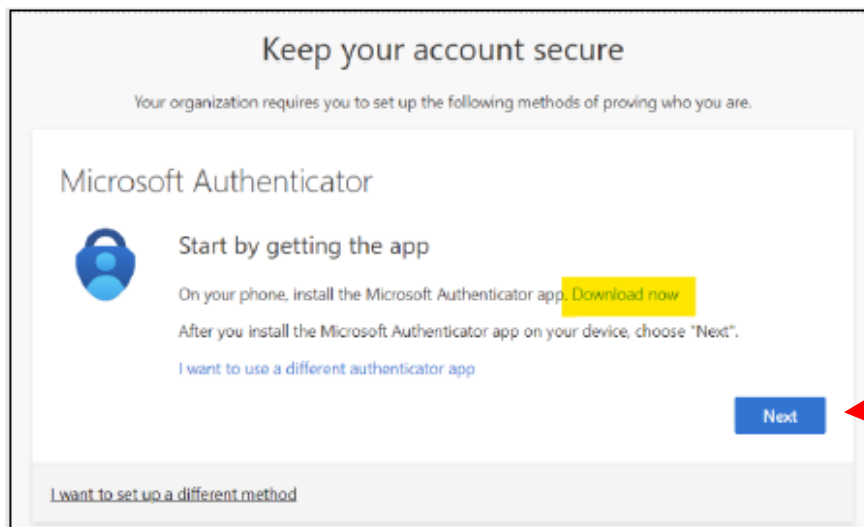
If a user needs their Multi-Factor Authentication (MFA) reset (i.e., has a new cellphone):

1. Send an email to dmhpasrr@umassmed.edu requesting that a ticket be opened to reset your MFA and explain the reason (e.g., new phone).

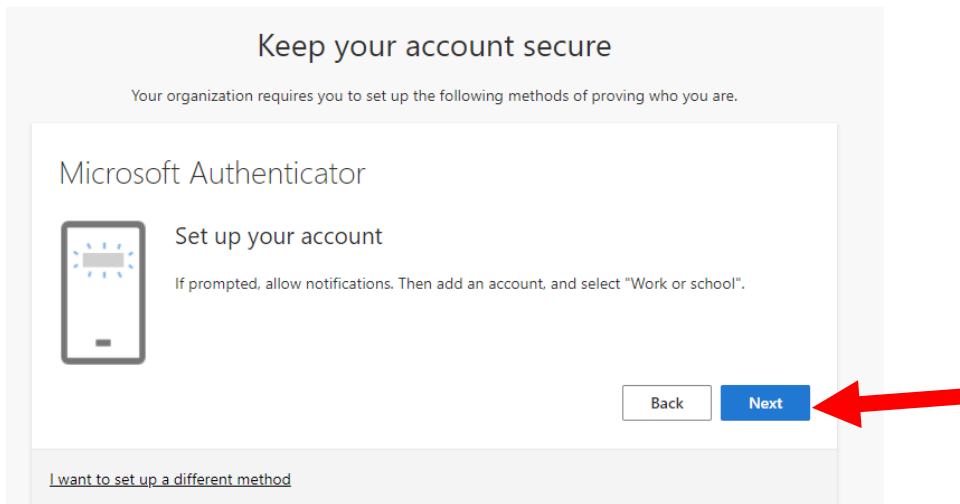
Provide your name, email address, and portal username.

Please note that your password will automatically be reset as well.

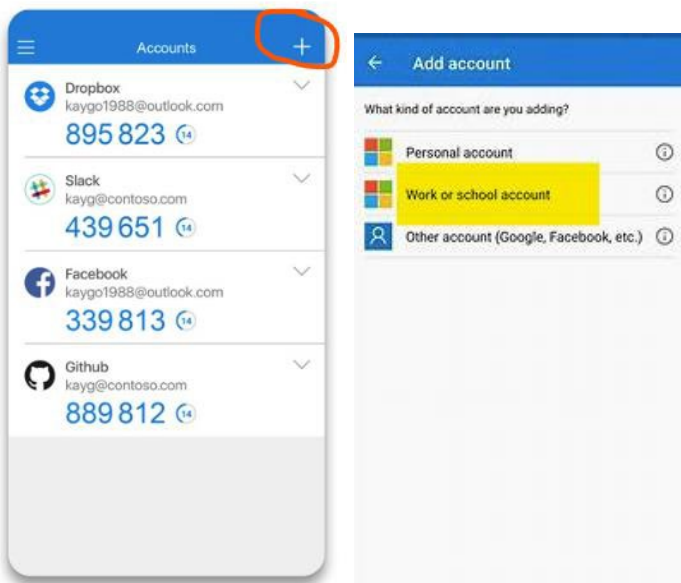
2. Download the Microsoft Authenticator app to your new phone through your app store.
3. Once UMass Chan IT resets the MFA and password, you will receive the new temporary password via secure email and can begin the login process:
 - Go to <https://www.masspasrr.org>
 - Enter your username (**masspasrr.org email that was provided to you**)
 - Enter the new temporary password you received.
4. You will see the following screen. Since you have already downloaded the app, please click on "Next":



5. Click "Next" again.



6. Open the Microsoft Authenticator application on your phone, click on the "+" symbol, and select "Work or School account."



7. Select “Scan QR code,” and using your phone’s camera, scan the code from the browser. Click “Next”.

The screenshot shows the 'Keep your account secure' page with the heading 'Microsoft Authenticator' and the instruction 'Scan the QR code'. A QR code is displayed in the center. Below the QR code is a button labeled 'Can't scan image?'. At the bottom right, there are two buttons: 'Back' and 'Next'. A red arrow points to the 'Next' button. At the bottom left, there is a link that says 'I want to set up a different method'.

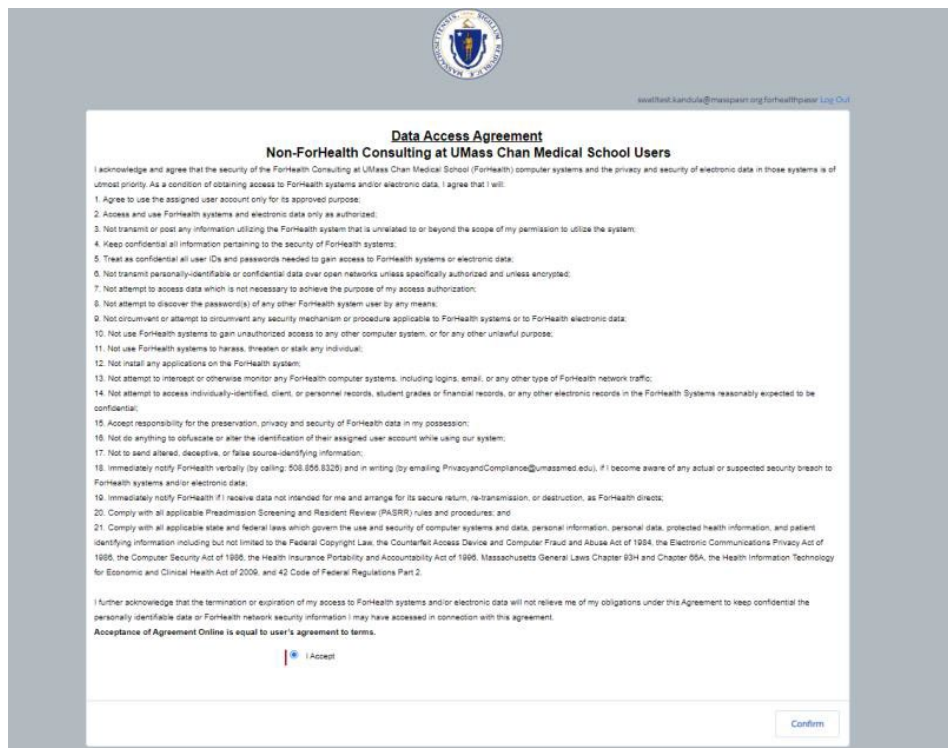
8. Enter the 2-digit number on your phone. Click “Next”, “Next”, and “Done”.

The first screenshot shows the 'Let's try it out' section with a progress bar and the instruction 'Approve the notification we're sending to your app by entering the number shown below.' The number '66' is displayed. Below the number are 'Back' and 'Next' buttons, with the 'Next' button highlighted by a red box. A link 'I want to set up a different method' is at the bottom left.

The second screenshot shows the 'Notification approved' status with a green checkmark and a notification icon. Below are 'Back' and 'Next' buttons, with the 'Next' button highlighted by a red box. A link 'I want to set up a different method' is at the bottom left.

The third screenshot shows the 'Success!' message: 'Great job! You have successfully set up your security info. Choose "Done" to continue signing in.' Below this, it says 'Default sign-in method:' followed by a lock icon and the text 'Microsoft Authenticator'. At the bottom right, there is a 'Done' button highlighted by a red box.

- The “Data Access Agreement” will be displayed. Review it and click “I Accept.” Then click “Confirm.”



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. Access and use ForHealth systems and electronic data only as authorized;
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 gain unauthorized access to any other computer system, or for any other unlawful purpose;
11. Not use ForHealth systems to harass, threaten or stalk any individual;
12. Not install any applications on the ForHealth system;
13. Not attempt to intercept or otherwise monitor any ForHealth computer systems, including logins, email, or any other type of ForHealth network traffic;
14. 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;
15. Accept responsibility for the preservation, privacy and security of ForHealth data in my possession;
16. Not do anything to obfuscate or alter the identification of their assigned user account while using our system;
17. Not to send altered, deceptive, or false source-identifying information;
18. Immediately notify ForHealth verbally (by calling: 508.855.8329) 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 Preadmission 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 Counterfeit Access Device and Computer Fraud and Abuse Act of 1984, the Electronic Communications Privacy Act of 1986, the Computer Security Act of 1986, the Health Insurance Portability and Accountability Act of 1996, Massachusetts General Laws Chapter 93H and Chapter 85A, the Health Information Technology for Economic 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.

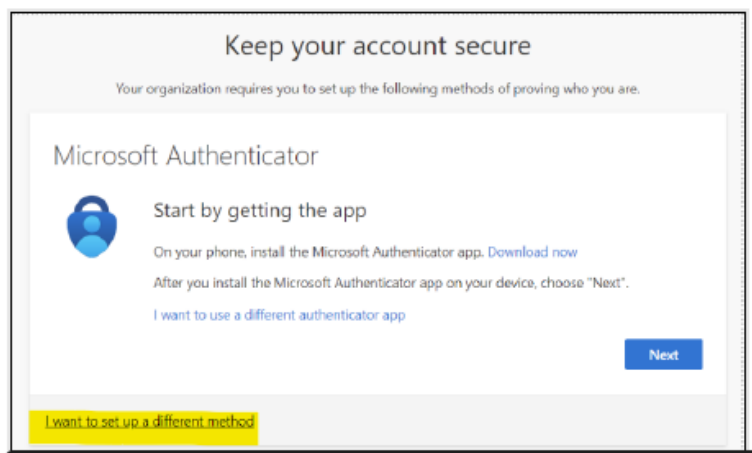
Acceptance of Agreement Online is equal to user's agreement to terms.

☐ I Accept

Confirm

If you do not want to download the app to your cell phone:

- Click on “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.

Microsoft Authenticator

Start by getting the app

On your phone, install the Microsoft Authenticator app. [Download now](#)

After you install the Microsoft Authenticator app on your device, choose "Next".

[I want to use a different authenticator app](#)

[Next](#)

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

2. 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 log in to the PASRR Portal. It must be a direct line.

3. Enter your phone number and select how you would like to authenticate, through text message or through a phone call, each time you access the PASRR Portal.

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

- B. 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?

United States (+1) [masked number]

☐ 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](#).

Next

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

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

A 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 [masked number]

Done

As in Step 9 above, the **“Data Access Agreement”** will be displayed. Review it and click on **“I Accept.”** Then click **“Confirm.”**