Fairview Multi-Factor Authentication Frequently Asked Questions

If you need assistance registering or setting up notification for multi-factor authentication (MFA) or self-service password reset (SSPR), please clink on these links:

- Information about MFA at M Health Fairview
- Information about SSPR at M Health Fairview.

You may also call Fairview's Technical Services Center at 612-672-6805 to speak with an agent.

1. What is multi-factor authentication (MFA)?

MFA is a method of authenticating a user through the use of two or more layers of independent credentials, also known as two-step verification. A user signs into their account from any enterprise approved device using their existing credentials and is then required to also authenticate via a second verification method such as mobile app verification, phone call, or text message. At this time, MFA affects anyone accessing a Fairview system from outside of the network (from an external location).

2. Why are we implementing MFA?

MFA enhances the security of accessing our IT systems from remote locations. Because you need to provide at least one additional factor other than User ID and Password to login, it helps to prevent bad actors from gaining access to our critical systems.

3. When would a user be required to enter MFA?

- Starting May 7, 2019, you may be required to provide a second layer of verification when logging in remotely to any M Health Fairview network service as this implementation is rolled out throughout the enterprise.

- MFA is not required if you are using Fairview managed (supplied) laptops, desktops, Fairview Cell phones, or shared kiosks connected to Fairview's trusted network.

4. What is considered remote access?

- Remote access means accessing Fairview systems from a site not on the Fairview network, using your home network, connecting from a coffee shop, or from a patient's home using the internet.
- If you work from home and log in to the Fairview network through Checkpoint VPN, or Secure Gateway, you will be required to enter MFA.
- Any time you log in via a mobile device such as an iPad or cell phone.
- Computers in the Clinics and Surgery Center will NOT require MFA.

5. If I do not have a Fairview.org email address will I still be able to register for MFA?

You will need to register with your Fairview ID followed by @fairview.org when prompted to enter an email address in the registration process.

- Your Fairview ID is what you currently use to access EPIC and Secure Gateway.
- Do not use any other email address when registering as this will not allow access to the Fairview Network.

6. What if my primary email address is @healtheast.org?

You will need to register for MFA using your HealthEast user ID @healtheast.org. Note: this is not the same as your HealthEast email address.

7. I am a legacy HealthEast user primarily using my legacy HealthEast account and also have a Fairview account, how will I access M Health Fairview applications when working remotely?

At this time continue to utilize RSA for logging into HealthEast Citrix or HealthEast VPN, from there open a browser and enter securegateway.fairview.org or other web application using your Fairview account without being challenged for MFA.

8. What are the methods for two-step verification?

There are three recommended methods of completing the two-step verification:

a. Method 1: Receive a code by text message on your phone to enter as part of your login.

b. Method 2: Receive a phone call with a voice message from Microsoft (usually 1-855330-8653), press # to complete the login process.

c. Method 3: Use the Microsoft Authenticator app, available for download on your personal mobile device.

Please note:

If you have a Fairview-provided mobile device, you may not able to download the Microsoft Authenticator app at this time. Use one of the first two methods listed above:

Code by text message or receive a phone call.

9. What if I use my personal cell phone to access Secure Gateway, Epic, or other M Health network service?

If you are using either cellular service or a guest network to access M Health Fairview network services this is considered remote access, you will be challenged to provide MFA.

10. What if I am in a "dead spot" or do not have cellular signal to my phone?

If you have downloaded the Microsoft authenticator application on your personal mobile device you will be able use the 6-digit code that refreshes every 30 seconds. This code will work even when there is no cellular signal to your phone.

- You will need to select "Authenticator app or hardware token – code" as your Default sign-in method on the "Security Info" page at aka.ms/mfasetup.

11. What if I am on an airplane and have internet access through the airline but no cellular service?

If you have downloaded the Microsoft authenticator application on your personal mobile device you will be able use the 6-digit code that refreshes every 30 seconds. This code will work even when there is no cellular signal to your phone.

- You will need to select "Authenticator app or hardware token – code" as your Default sign-in method on the "Security Info" page at aka.ms/mfasetup.

12. What if I already use the Microsoft Authenticator app for another account, do I still need to register with M Health Fairview?

If you have downloaded the Microsoft authenticator application on your personal mobile device for use with another account, you will need to register/add your Fairview account as well.

- Follow on screen instructions for adding an account to the authenticator application on your mobile device.

13. Can I use the office phone option as a method of two-step verification?

Using your office phone for verification is not a supported method for MFA across the enterprise at M Health Fairview; even though the option may appear on the Microsoft additional security verification setup screen. This option is not helpful because MFA is only challenged when you are connecting outside of the Fairview Network and trying to access Fairview systems remotely.

14. What type of mobile device can I set up the Microsoft Authentication App on?

You can set it up on any iOS or Android device as described in the MFA registration instructions.

15. What if I am not able to receive the notification on my mobile device?

When setting up the security information, you will provide alternative methods of notification to use in case your default method fails to work.

- In this scenario you will need go to aka.ms/mfasetup and change your "Default method to signin" to one of your alternate methods.

- When challenged for MFA to log in to aka.ms/mfasetup, use the "Having trouble? Sign in another way" to complete the log in.

16. What if I temporarily lose the phone that I have set up for two-step verification?

When setting up the security information, you will provide alternative methods of notification to use in case your default method fails to work.

- In this scenario you will need go to aka.ms/mfasetup and change your "Default method to signin" to one of your alternate methods.

- When challenged for MFA to log in to aka.ms/mfasetup, use the "Having trouble? Sign in another way" to complete the log in.

- If you have lost your phone and are not able to use one of the alternate methods call the *M Health Fairview Technical Service Center* at (612)-672-6805.

17. What if I get a new phone – how do I transfer my account to the new phone?

- Go to aka.ms/mfasetup to begin log in with your credentials - you will be challenged for MFA to log in. (you will not be able to complete the log in)
- Next to "having trouble?" Click "Sign in another way"
- Assuming you kept your same number – choose call (your number listed)
- Answer the call and listen to the message and click # at the end to verify its you.
- Once you have completed the authentication the Security Info page will be displayed
- Delete your "old" Microsoft authenticator and click on +Add Method
- Follow the on-screen prompts and it will advance to a page with the QR code displayed
- Scan the QR code with your new phone and complete set up

18. How do I check if the Microsoft Authenticator app and authentication phone numbers are registered for two-step verification?

- Go to aka.ms/mfasetup and review the information on the "Security Info screen.