

MFA - Frequently Asked Questions

1. Why do I need MFA?

With the rise of cyberattacks, including public health organizations, it is important that we protect our systems from potential network threats. Ignoring this can lead to a breach of patient data and privacy. Multi-factor authentication creates an added layer of security to access NYGH network and services and so is helpful to ensure that the system is secure.

2. How long does this take?

Setting up MFA typically takes 5 minutes. Please refer to our guide- 'How to Set-up Multi Factor Authentication for an easy step by step walkthrough on how to set-up MFA

3. Is this only for remote users?

While the initial roll-out is for remote users, eventually all NYGH staff and contractors will need to be MFA set-up on their accounts. This is part of the protocol for new hires as well, across departments.

4. Do I need to keep authenticating myself each time I log in?

Not actually. Microsoft has a provision for an access point - device to be remembered on the network for 90 days. You can select this option the next time you are asked to provide access authentication.

5. What if I lose my mobile phone?

You can always change your authentication mode (please refer to document 'How to Modify your MFA Preferences'). In this case, you can select authentication phone and enter an alternate number. Once you get your phone back, we encourage you to reactivate the mobile app.

6. What happens if I lose my network coverage at some point?

Microsoft Authenticator app does not require cell phone or Wi-Fi network to generate passcodes.