Multi-Factor Authentication for Accessing Citrix Outside of Memorial Health
Frequently Asked Questions

Q What is MFA (Multi-Factor Authentication)?

A MFA is an additional authentication method that takes place when a colleague attempts to sign in. It requires a second form of identification in addition to the provider's username and password combination.

Q How will I get the "second factor?"

A In MH's current state, the six-digit code will be texted to the provider's registered cellphone. Or an enrolled smartphone with Microsoft Authenticator application installed will provide the six-digit code.

Q Why do we need to do this?

A The primary reason is to strengthen MH's security posture. Healthcare is one of the top targets for cyber criminals, and as part of Memorial's defense in-depth strategy, requiring MFA ensures those who gain access to the enterprise environment are who they say they are.

Q What options do I have to receive my MFA code?

A There are two options. First is a text to a registered phone number and second is utilizing Microsoft's Authenticator application.

Q Where will I be required to use MFA?

A You will be prompted for MFA when attempting to connect from a remote location outside of a Memorial Health facility (home, Starbucks, etc.).

Q What options do I have if I don't have a smartphone?

A You can request a phone call, text message, email or use the Authenticator app. If you don't have a smartphone, but you do have a landline phone, you could receive the code via a phone call.

Q If I elect to receive text messages, will it be from MH or another number?

A The sending number will be random, but the structure of the message will be like this.