Multi-Factor Authentication (MFA) Frequently Asked Questions

This guide provides answers to common questions about logging in, setting up, and managing Multi-Factor Authentication (MFA) for the HealtheConnections Health Information Exchange (HIE) portal. It is designed to help authorized users quickly resolve issues and ensure secure, seamless access.

The quick links below allow users to jump directly to the sections most relevant to their needs.

About Multi-Factor Authentication (MFA) 2
- What is Multi-Factor Authentication (MFA)? 2
- Why is MFA required? 2
- Why isn't a primary authentication enough (e.g., a password)? 2
- What are the benefits of MFA? 2
- What is Okta? 2

HealtheConnections MFA 2
- Which MFA methods does HealtheConnections support? 2
- Do I need to set up MFA again if I registered previously? 2
- Can I turn off MFA? 2
- Can I register more than one device for MFA? 2
- How do I set up and register my MFA? 2
- How do I register a new device or change my MFA method? 3
- What if I'm stuck on the "Enrolling Your Device" screen? 3
- Why do I keep seeing MFA prompts after selecting "Do not challenge me on this device again"? 3
- How many attempts do I have until I am locked out of my account? 3

MFA Account Troubleshooting 3
- What if I forgot my password or am locked out of my account? 3
- How do I re-enroll in MFA? 3
- How do I contact HealtheConnections? 3

For help or additional information, contact HealtheConnections.

443 North Franklin St., Suite 001
Syracuse, NY 13204

About Multi-Factor Authentication (MFA)

What is Multi-Factor Authentication (MFA)?

MFA is an authentication method that requires two sources of verification to access a digital resource. It helps protect against unauthorized access by ensuring that users are who they claim to be.

Why is MFA required?

MFA provides enhanced security beyond traditional usernames and passwords, which are increasingly vulnerable to phishing, brute force attacks, and other cyber threats. MFA adds an additional layer of protection to ensure the security of sensitive information.

Why isn't a primary authentication enough (e.g., a password)?

Passwords are difficult to manage and vulnerable to attacks such as phishing and social engineering. If compromised, a password alone can give hackers access to all resources associated with the account. This poses a particular risk for users with privileged information.

What are the benefits of MFA?

- Reduces the risk of identity compromise.
- Adds peace of mind knowing sensitive patient data is better protected.
- Encourages mindfulness in authentication by reinforcing the importance of security.

What is Okta?

Okta is a software platform that helps organizations manage secure digital access.

HealtheConnections MFA

Which MFA methods does HealtheConnections support?

- Okta Verify app
- Google Authenticator
- Email authentication
- FIDO2 WebAuthn

Do I need to set up MFA again if I registered previously?

No. Once configured, MFA does not need to be set up again unless you are changing or resetting your methods (e.g., new email address).

Can I turn off MFA?

No. MFA is required for all accounts and cannot be disabled.

Can I register more than one device for MFA?

No. You cannot register multiple devices, tokens, or emails for a single account. You may, however, select two or more MFA methods.

How do I set up and register my MFA?

For new authorized users:

1. Follow the steps and guidance provided in HealtheConnections onboarding emails.
2. Access the HealtheConnections HIE portal.

443 North Franklin St., Suite 001
Syracuse, NY 13204
healtheconnections.org

3. Upon logging in, a redirect will appear to complete MFA setup and registration.
4. Select and submit the preferred MFA method(s).
5. After completion, a redirect will return the session to HealtheConnections.
6. Log in with HealtheConnections credentials to begin using the portal.

For existing authorized users:

1. Contact HealtheConnections to reset your MFA. Once reset follow the steps below:
    a. Access the HealtheConnections HIE portal.
    b. A redirect will appear to complete MFA setup and registration.
    c. Select and submit the preferred MFA method(s).
    d. After completion, a redirect will return the session to HealtheConnections.
    e. Log in with HealtheConnections credentials to resume portal use.

How do I register a new device or change my MFA method?

Contact our Support team at 315-671-2241 x5 or support@healtheconnections.org.

What if I'm stuck on the "Enrolling Your Device" screen?

If you are stuck in a loop duringemail enrollment, or are not receiving codes or push notifications, your device may not have enrolled correctly. Contact our Support team at 315-671-2241 x5 or support@healtheconnections.org.

Why do I keep seeing MFA prompts after selecting "Do not challenge me on this device again"?

This is often a cookie management issue. The choice is stored in a browser cookie. If you clear cookies or switch to a new browser, the setting will not be remembered.

How many attempts do I have until I am locked out of my account?

After three failed attempts, your account will be locked, and you will be prompted to reset your password.

MFA Account Troubleshooting

What if I forgot my password or am locked out of my account?

To reset a password or unlock an account, utilize the self-service options located below the Sign in button. Select the appropriate link (Forgot password or Unlock Account) and follow the on-screen prompts.

If you have questions or need assistance, contact our Support team at 315-671-2241 x5 or support@healtheconnections.org for assistance.

How do I re-enroll in MFA?

Contact our Support team at 315-671-2241 x5 or support@healtheconnections.org for assistance.

How do I contact HealtheConnections?

HealtheConnections is here to help and is your first stop for support. For questions or assistance, please contact HealtheConnections at:

- 315-671-2241 ex. 5
- Support@healtheconnections.org

443 North Franklin St., Suite 001
Syracuse, NY 13204
healtheconnections.org