Multi-Factor Authentication for CyncHealth Clinical Viewer Users

Frequently Asked Questions

Background

To provide the highest levels of security for participants, CyncHealth is instituting multi-factor authentication (MFA) to access the Clinical Viewer.

Below are some key questions end users commonly have.

Frequently Asked Questions

Q: ***Why is CyncHealth moving to MFA?***
A: Healthcare entities, data companies, and others are under constant security attacks. We are implementing greater security protocols to protect all CyncHealth participants, and the CyncHealth IT infrastructure from bad actors and other external threats.

Q: ***Can I keep using [my/the] old bookmark to access the clinical viewer?***
A: Although it will appear that you can use the old site, the system will prompt you to go to the new site. The new site is https://secure.cynchealth.org.

Q: ***What will happen if I don't enroll in MFA?***
A: Users who do not enroll in MFA will not be able to access to the Clinical Viewer.

Q: ***What do I need to do on the day of the transition to MFA?***
A: You will login to the Clinical Viewer as usual on the day we transition to MFA. The system will prompt you to set up a new account, in which you will automatically receive an email asking to create a unique password and desired second authentication method. From that point on, you will simply use the new URL to access the Clinical Viewer. The new site is https://secure.cynchealth.org.

Q: ***What is the new URL for the clinical Viewer that I need to bookmark?***
A: The new URL is https://secure.cynchealth.org.

Q: ***Does this affect CyncHealth SSO Integrations with EHR's such as Epic and Cerner?***
A: No, this does not impact EHR integrations. If you would like to discuss the possibility of integration, please contact us at support@cynchealth.org.

Q: ***What is the recommended MFA method?***

A: There are multiple options, we recommend your facility leadership determine how the organization will setup MFA. You can use:

Mobile Apps (push notifications)

- Okta Verify
- Google Authenticator

Other Methods:

- SMS Text Messaging
- Email

You should discuss this with your facility's IT Leadership and/or Designated User/Authorizer. Your organization's policy may dictate which method to use.

If needed, the URLs to navigate to the Okta Verify app (case sensitive):

- *Apple: https://apple.co/37c5QL2*
- *Android: https://bit.ly/3KtHxql*

Q: ***Do I need an iPhone/Android/smartphone or a data plan to use MFA?***

A: No. You should discuss what MFA method to use with your facility's IT lead and/or Designated User/Authorizer. Your organization's policy may dictate which method to use.

If you are using the Okta Verify app for MFA then you will need an iPhone or Android phone. However, it is also possible to enroll to receive SMS passcodes and emails if your organization permits it.

Q: ***Do I have to install Okta Verify on my iPhone/Android/smartphone?***

A: No. Okta Verify is just one of several methods to achieve multifactor authentication. Okta Verify and Google Authenticator are mobile apps that generate passcodes for login and aloe for push notifications for easy, one-tap authentication on your mobile device.

*You should discuss what MFA method to use with your facility's IT lead and/or Designated User/Authorizer. Your organization's policy may dictate which method to use.

If needed, the URLs to navigate to the Okta Verify app (case sensitive):

- *Apple: https://apple.co/37c5QL2*
- *Android: https://bit.ly/3KtHxql*

Q: ***If I choose to use a mobile app, how much data does it use?***
A: Mobile app authentication requests require a minimal amount of data -- less than 2KB per authentication. For example, you would only consume 1 megabyte (MB) of data if you were to authenticate 500 times.

Q: ***I use a mobile app for MFA and I got a new phone, and/or lost my phone. What should I do?***
A: Please contact the CyncHealth IT help desk at support@cynchealth.org or call 402-506-9900 Option 1, CyncHealth support will remove your old device and assist you with enrolling your new device.

Q: ***Can mobile apps see my password?***
A: No. Your password is stored encrypted. Mobile apps cannot see your password.

Q: ***Do mobile apps give up control of my smartphone?***
A: No. The mobile apps have no access to change settings or remotely wipe your phone. Mobile apps require minimum visibility to your smartphone. Basic information such as supported operating system level and serial number.

Q: ***Will I be required to use MFA when accessing the Clinical Viewer from inside the facility I work at?***
A: If your facility meets the requirements, a Static IP can be used for the second portion of the MFA. This alleviates the need for a second factor while onsite at your facility. Please have your IT administrator complete the Static IP Form located here.

If your facility does not have a static IP, inquire with your IT department/partner to understand if a static IP is an option at your facility.

If you organization does not have a static IP, yes you will be required to use MFA each time you access the Clinical Viewer

Q: ***I am a Designated User. Will I still create and terminate users for my organization?***
A: Yes. The Designated User process will not change. Designated users will still use the URL: https://hie.nebex.org/csp/HSPS/UMP/UI/userlist to create and remove active users.

Q: ***Will Designated Users still need to assist with changing passwords?***
A: No. Password resets will be managed by the MFA application. Any issues not able to be handled by the self-service password reset process will need to be escalated to support@cynchealth.org.

Q: ***I am a Designated Authorizer. Will I still make requests for creation and termination of users for my organization?***

A: Yes. The Designated Authorizer process will not change. Designated Authorizers will still make requests for access for their users following the support ticket creation process https://nehii.teamdynamix.com/TDClient/2292/Portal/Requests/TicketRequests/NewForm?ID=f1iLxVAcXlg_