

KEEPING YOUR DATA SAFER WITH MULTI-FACTOR AUTHENTICATION

The Children's Hospital Association requires you to use multi-factor authentication (MFA) to access our data programs and systems. You will set up an MFA on the Okta User Dashboard, which you will access using your CHA sign-in credentials.

We've provided several ways to set up MFA. You may use any one or a combination of methods to access your CHA account, depending on your needs and workflow.

If you experience difficulties, please contact the [Help Desk](#).

Okta Verify

The Okta Verify app helps protect your data, ensuring only you can access your accounts. You will configure the app when logging into your CHA account.

- Log in to your CHA account.
- Click *Setup* located under the Okta Verify option.
- Follow the prompts to access your Okta User Dashboard and obtain a QR code.
- Download and install Okta Verify on your mobile device (phone or tablet) from either the Google Play Store or the Apple App Store.
- Using your mobile device, scan the QR code displayed on your computer screen.

Once you've set up Okta Verify, you'll be prompted to send a push notification to your device any time you access your CHA account. Tapping the push notification on your device will allow access to your account.

Google or Microsoft Authenticator

This option allows you to use a third-party app to verify your identity.

- Go to the Apple App Store or Google Play Store and install the Google or Microsoft Authenticator on your mobile device.
- When signing into your CHA account, select the Google Authenticator option. This option works for the Microsoft Authenticator app, too.
- Select your device type, and then click *Next*.
- Launch your authenticator app.
- Tap the $\neq$ sign.

- Tap *Scan a QR Code* and point your device camera at the QR code displayed on your computer's browser. Your camera will scan the QR code automatically.
- In your computer's web browser, click *Next*.
- In the *Enter Code* field, type the setup key shown in Google or Microsoft Authenticator on your mobile device.
- Click *Verify*.

If your device can't scan QR codes, click *Can't Scan* located under the QR code and follow the prompts.

Email Authentication

Each time you log in, you can request an authentication message be sent to your primary email address to verify your identity. The email will contain a "magic link" or a six-digit passcode you will enter on the log-in page. These links or passcodes have a limited lifetime. If the link or passcode are not used within this time frame, you will not be authenticated.

Authentication emails may arrive in your spam or junk folder. Please check these folders if your message does not arrive.

Security Key or Biometric Authenticator

This factor authenticates using a biometric method, such as fingerprints or facial recognition. You can use options including security keys, such as YubiKey or Google Titan, or integrated platform authentication, such as Windows Hello or Apple Touch ID.

- Sign into your CHA account.
- Select the Security Key or Biometric Authenticator option.
- Okta will ask for information about the option you wish to use.
- Once confirmed, the security key or authenticator will appear in the *Extra Verification* section of the *Settings* page.

You set up a maximum of 10 security keys and biometric authenticators. Please note that biometric authentication must be set up separately on each device you intend to use.

Security Question

The Security Question factor prompts you to enter a correct response to a question you have selected from a list of possible questions.

- Upon logging into your CHA account, click *Setup* under the Security Question option. This will take you to the Okta User Dashboard.
- Click your name in the upper right corner and select *Settings*.
- In the *Extra Verification* section, click *Set Up* beside *Security Question*. You might need to authenticate again.
- On the Set Up Multifactor Authentication page, click *Setup*.
- Select a question from the dropdown list and type the answer in the *Answer* field.
- Click *Save*.

Security Questions must meet the following guidelines:

- Must be at least four characters long.
 - Can't be your password or username.
 - Can't be included in the question.
-

SMS Authentication

When signing into your CHA account, select the SMS Authentication option.

- Select the country where your phone number is registered from the dropdown list.
- Enter your phone number in the *Phone Number* field. Leave out any dashes and the leading zero if your country's phone system uses them.
- Click *Send Code*.
- You will receive a code in an SMS message.
- Type the code in the *Enter Code* field.