Two-Factor Authentication (2FA) FAQ

Last modified on 02/26/2025 11:12 pm EST

Turn on two-factor authentication (2FA) to protect your DrChrono account.

What is two-factor authentication (2FA)?

Two-factor authentication (2FA) is a security measure that safeguards your login credentials. Your mobile device is linked to your login credentials and used to generate or receive an authentication token, which you must enter while logging in. 2FA adds an extra layer of security, requiring a malicious user to obtain both your login credentials and access to your mobile device to access your account.

2FA is available on all plan types for provider and staff accounts.

What is two-factor authentication?

2FA adds an extra layer of security to your account by requiring your password and a second verification form to access it. This typically involves receiving a unique code on your mobile device or email that you'll need to enter along with your password when logging in.

Why should I turn on 2FA?

Turning on 2FA significantly enhances the security of your account by reducing the risk of unauthorized access, even if your password is compromised. It safeguards against phishing attempts and other security threats, protecting sensitive patient data.

What can I use to receive the second authentication factor?

Only the mobile version of the Authy app is authorized for use with DrChrono 2FA.

Do I need to enter the second authentication factor every time I log in?

Yes. For security purposes, you must enter the second authentication factor every time you log in to your DrChrono account from a new device or browser or after a certain period of inactivity. When you enter your Authy two-factor token code, you see an option to save the token for 30 days.

What if I lose access to the device or method used for the second authentication factor?

It's essential to keep your backup codes or alternative authentication methods in a secure place.

Can I turn off 2FA if I no longer want to use it?

Yes. You can turn off 2FA in **Account Settings** > **Security**; however, we recommend you keep it on for enhanced security.

How do I set up 2FA?

How do I set up Two-Factor Authentication (2FA) in my account?

How do I set up Two-Factor Authentication (2FA) for a staff member?

How do I use 2FA?

How does Two-Factor Authentication (2FA) work in DrChrono?