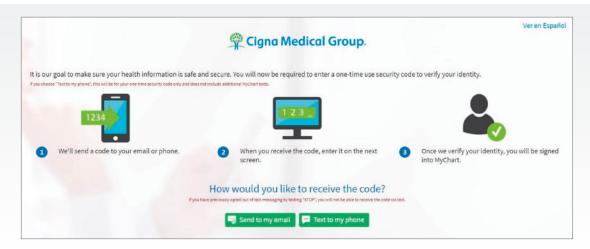# TWO-FACTOR VERIFICATION

How to use MyChart Two-Factor Verification

Two-factor verification is an additional level of security on top of a user's password. A one-time code can be sent to a user's email or mobile phone. The user must enter this code before they can log in to view their private heath information.

Click **"Send to my email"** or **"Text to my Phone"**.

Enter the code you receive in the email or test on the MyChart security code prompt.

You will not be prompted again if you select the remember me box (180 days for mobile and 90 on desktop).

If you choose "Text to my phone" the code will be sent to your mobile.

Helpful Tip:
If using email, be sure to open a new browser tab when retrieving your code.

Patient FAQ for MyChart login page

What is Two Factor Verification?

It is a method of confirming users' claimed identities by using a combination of two different factors. This would be something they know (password) and a second factor (token) which is a six digit number.

Why Should I use Two Factor Verification?

To provide additional security during MyChart signup, login, and password reset or expiration workflows. Minimizes identity theft and helps prevent disclosure of your electronic health information.

How does Two Factor Verification work?

When two factor verification is used, after a patient enters their MyChart username and password, the patient is taken to the Additional Security Verification page where they can have a code emailed or texted to their mobile phone. After the patient receives the code, they can enter it to finish logging into MyChart.

Do I need to use Two Factor Verification every time I log in to MyChart?

Yes, unless you indicate this is a private device; and skip this step next time. If you indicate this is a private device you will not be promoted for 90 days with mobile or 180 days with desktop.

Cigna Medical Group