801 Gateway Blvd., Suite 100 | South San Francisco, CA 94080
www.hpsm.org

HPSM Provider Portal Two-Factor Authorization FAQ

Starting February 21, 2023, the Health Plan of San Mateo (HPSM) provider portal will require two-factor authentication for the HealthTrio member and provider portals. This will align HPSM with best practices for security and add an extra layer of protection to the portal. This document should help providers answer some frequently asked questions (FAQs) about two-factor authentication in our portals.

Log into the provider portal here: **https://www.hpsm.org/provider/portal**

What is two-factor authentication?

Two-factor authentication, or 2FA, is an extra layer of protection used to ensure the security of online accounts beyond just a username and password. Enabling 2FA will put us in line with industry standards of security and help ensure our members and providers accounts are not accessed by malicious actors.

How will this effect members and providers?

Effective February 21, 2023, providers will need to set up an email or cell phone number in the portal to use for 2FA.

How do I set up two-factor authentication?

Here are the steps a provider will take to set up two-factor authentication:

1. Visit **https://www.hpsm.org/provider/portal**.
2. Starting February 21, 2023, providers will be asked to set up an email or cell phone number in the portal for two-factor authentication.
3. HPSM providers will then check their phone number or email, where they will have received a six-digit code to log into the portal.
4. Providers can then enter that six-digit code into the portal to access their account.
5. There is an option to “remember” the device the provider is using for 24 hours; this means they will not need to use 2FA again until the next day.

What will the two-factor authentication message say when I receive it?

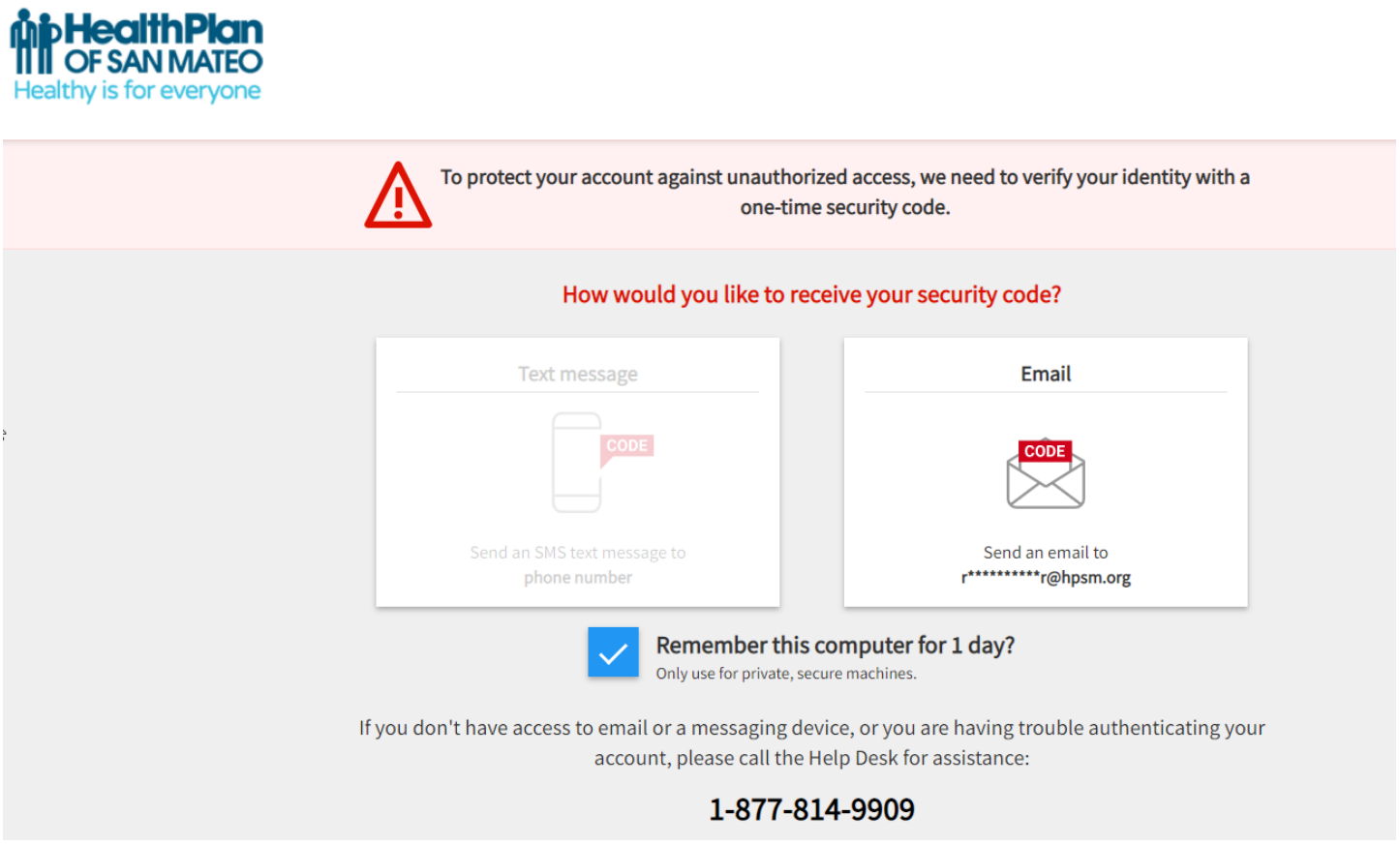
The two-factor authentication message will be different depending on how you sign up for the portal.

1. If the provider uses an email as their authentication method:
    a. They will be sent an email from **no-reply@healthtrio.com**.
    b. The subject of the email will be "Your account security code."
    c. The message will read "Please use security code ###### to log in to your health plan portal account."
2. If the provider uses a cell phone as their authentication method:
    a. They will be sent a text message from **870-729-8620**.
    b. The message will read "Please use security code ###### to log in to your health plan portal account."

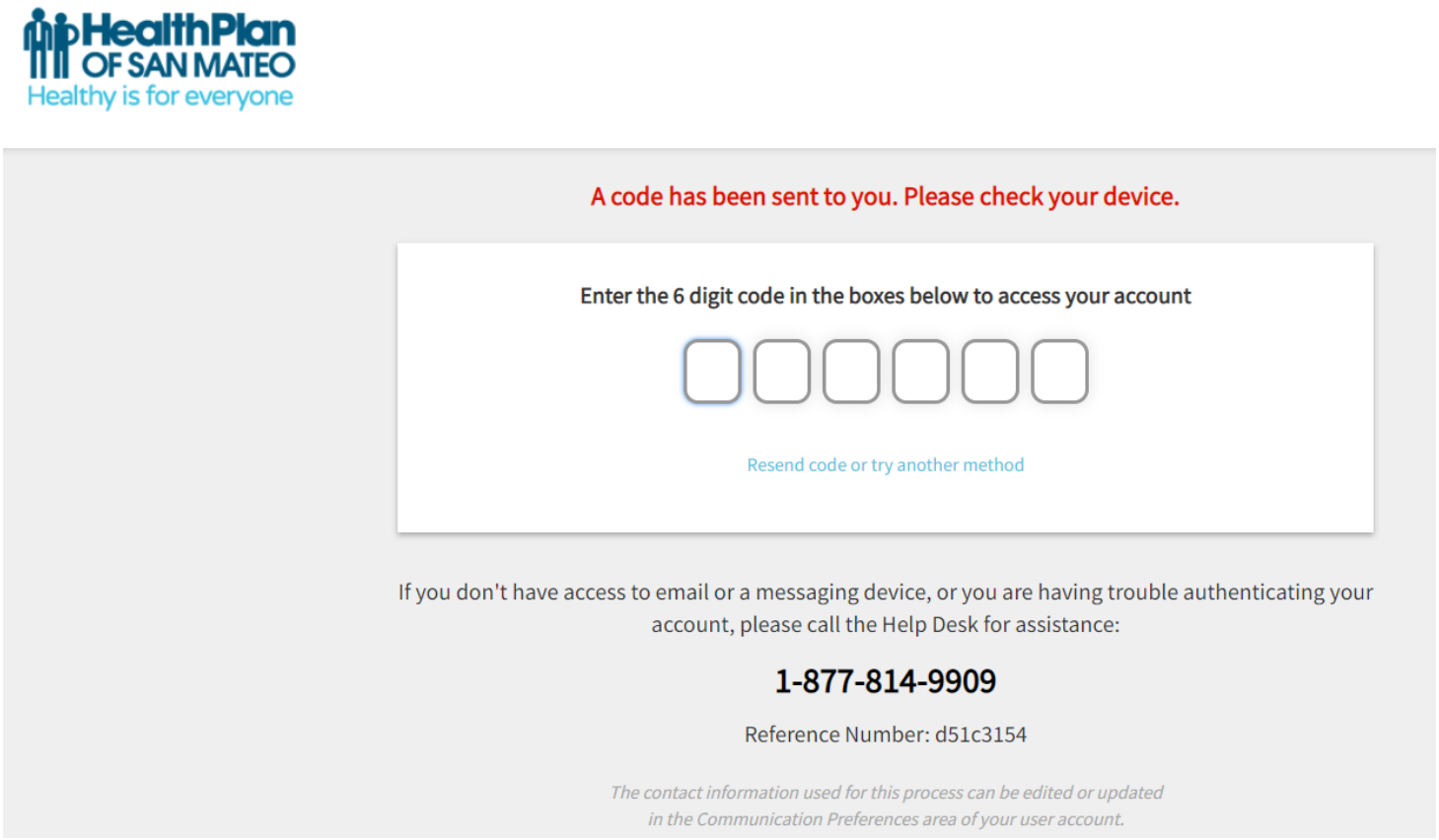
We are unable to customize the message that providers receive but we want to be able to assure users that this is not a scam email/text message.

Screenshots

Select 2FA method



Enter code



Confirmation