

**An Important Message from
The Texas Health and Human Services Commission (HHSC)**

**ALERT for STEPS Providers: Be Aware of Email
Phishing Scam Using HHSC PFD Logo**

HHSC learned of a phishing attempt targeting State of Texas Electronic Providers (STEPS) primary entity contacts. The phishing email asks recipients to verify their information and sign a document. It also states that recipients may be penalized if they do not respond.

STEPS Providers have received emails from sources pretending to represent the HHSC Provider Finance Department (PFD). The phishing emails include the following information:

- **Sender:** donnafulfer839@gmail.com
- **Subject Line:** Primary Entity Contacts and STEPS Access Information

Phishing is a common type of cyberattack that uses email or text messages to acquire sensitive information, such as email passwords. These messages are often designed to appear as though they come from a trusted person or organization. They may attempt to persuade recipients to open malicious links or enter information on fake websites.

The recent emails include the HHSC PFD logo to make the sender appear legitimate. Each email asks the recipient to confirm information, click on a button or link, and enter sensitive information in a location provided by the sender. The email also threatens to suspend or revoke the provider's license. Some recipients may believe this threat refers to their Medicaid license or contract. This email is fraudulent, so licenses and/or contracts will NOT be suspended or revoked if providers do not respond.

HHSC PFD did not send these emails. STEPS providers should not respond to the emails, click any links in them, or provide sensitive personal or business information.

How to Verify Official HHSC Communications

To verify that you are communicating with HHSC PFD:

1. **Check the Domain.** Official emails are sent from the “gov” domain.
 - **Note:** Although the sender's name can be falsified, the email address in brackets, such as “name@hhs.texas.gov,” must match the HHSC domain.
2. **Review STEPS Portal emails.** Automated notifications from the STEPS Portal may also come from “noreplypfdsteps@hhs.texas.gov.” If you are unsure whether an email is legitimate, do not click any links. Navigate directly to the portal using a saved bookmark.
3. **Hover before clicking.** Before clicking a link, hover over it to view the destination. If the link does not lead to a “.texas.gov” domain or an approved portal site, **do not click.**

When reviewing an email for authenticity, look for the following signs of phishing:

- Includes a suspicious sender's address that may imitate a legitimate business or government entity.
- Demands urgent action.
- Uses a generic greeting or signature.
- Excludes contact information from the signature block.
- Uses linked text that does not match the destination displayed when you hover the link.
- Contains spelling, grammar, or sentence-structure errors.
- Uses inconsistent formatting.
- Includes a suspicious attachment(s) and asks you to download or open it.

If you are a STEPS provider and receive an email claiming to be from HHSC PFD, contact HHSC PFD to verify the email's authenticity.

If you received such an email and clicked a link or provided sensitive information:

- Report it to your organization's information technology department.
- Reset your passwords.
- Scan your computer or device for viruses or malware.

Questions?

If you have questions, please contact UnitedHealthcare Customer Service at 888-887-9003, 8 a.m.–6 p.m. CT, Monday–Friday.