An Important Message from

The Texas Health and Human Services Commission (HHSC)

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

The Texas Health and Human Services Commission (HHSC) learned about a phishing attempt related to the state fiscal year 2027 enrollment.

HHSC is aware that QIPP Providers have received emails from sources pretending to be the HHSC Provider Finance Department (PFD). These emails, referred to as phishing emails, have been sent using the following information:

- **Fake Sender**: awashington@rootedschool.org
- **Email Subject**: IMPORTANT: Verification for Primary and Secondary Contacts for the QIPP Submission Portal

Phishing is a common type of cyber-attack that targets individuals through email or text messages to attempt to acquire sensitive data, such as email passwords. These messages are often designed to look like they come from a trusted person or organization, to get recipients to open malicious links or enter information on malicious websites.

The recent emails contain the HHSC PFD logo to make the sender appear valid. Each email asks the recipient to confirm information, click on a button or link, and to enter sensitive information in a location that the fake senders provide. The email also threatens to suspend or revoke the provider's license, which some readers may believe refers to their Medicaid license or contract. However, it does not.

The emails were not sent by HHSC PFD – Providers should not respond to them, click on any links in them, or send sensitive personal or business information.

How to Verify Official HHSC Communications

To ensure you are communicating with the real HHSC Provider Finance Department, please note:

1. **Check the Domain:** Official emails are sent from the **texas.gov** domain.
    - *Note:* While the sender's *name* can be faked, the email address between the brackets (e.g., [**name@hhs.texas.gov**]) must match our domain.
2. **Hover Before You Click:** Before clicking any link, hover your mouse over it to see the actual destination URL. If it does not lead to a .texas.gov or approved portal site, (iamonline.hhs.state.tx.us), **do not click.**

When reviewing emails for authenticity, look for the following cues to help identify phishing emails:

- Includes suspicious sender's address that may imitate a legitimate business or government entity.
- Demands you take urgent action.
- Offers a generic greeting or signature. Excludes contact information from the signature block.

- Spoofs hyperlinks and websites in body text that does not match the URL text shown when hovering over links.
- Contains spelling errors, poor grammar, or poor sentence structure. Uses inconsistent formatting.
- Includes suspicious attachments with requests for you to download and open the attachment.

If you are a provider and receive an email that claims to be from the HHSC PFD, and you are concerned about its authenticity, you may contact HHSC Provider Finance Department to verify the email's validity.

If you received such an email and have already clicked on the link or provided sensitive information, we encourage you to report it to your organization's information technology department, reset your passwords, and scan your computer/device for malicious viruses/malware.

Questions?
For additional questions, please contact **UnitedHealthcare Customer Service at 888-887-9003, 8 a.m.–6 p.m. CT, Monday–Friday.**