Temporary Working from Home Guidance during COVID-19 Coronavirus

Follow these guidelines based off of UnitedHealth Group Policies and Procedures to keep our company's information safe and secure while temporarily working from home. This document does not replace the UnitedHealth Group Human Capital Telecommuting Policy.

Workspace

- Use your UnitedHealth Group approved computer and connect via the UnitedHealth Group approved Virtual Private Network (VPN) for work. If an approved computer is not available, then employees may connect through Citrix using Two-Factor Authentication.
- The company understands that you may have to accommodate family members and create a temporary workspace. Do your best to keep your workspace separate in order to maintain the confidentiality and privacy of health information.
- Place your laptop in a way where others are unable to view information on the monitor from outside or from the street.
- Ensure voice-activated smart devices or digital assistants such as an Alexa, Google Home, etc. are turned off, or in a separate room far enough away from your dedicated workspace so it is not activated by an unintentional voice prompt.
- Maintain a clean and clear desk and secure protected documents when unattended. Always check your desk and printer (if you have an approved printer you are using for UnitedHealth Group) prior to leaving the workspace.

Laptop and Tablets

- Lock your computer by using Ctrl+Alt+Del and select 'Lock Computer' or the Windows key and 'L', and remove your Smart Card or Yubikey whenever you step away from your computer for a break and/or when you are done working for the day.
- Ensure your laptop is secure if you are not at home, such as placing it in a locked drawer or file cabinet and locking your doors.
- Laptops and tablets must not be left unsecured (e.g. at a hotel, while traveling, unattended in a vehicle, etc.).

Documents

- Ensure that you keep documents as secure as possible while in your temporary work space and bring everything back to the office when it is permissible to return.
- If possible, keep documents containing Protected or Confidential information at the office.
- Documents that contain Protected or Confidential information are to be shredded when they are no longer needed.

Remain Vigilant and Take the Following Precautions

Attackers are taking advantage of COVID-19 concerns by running phishing scams. These scams include emails asking you to download important information about the virus, getting access to brand recognized sites for gathering of personal information, and fraudulent donation campaign sites.

To stay vigilant:

- Check the sender's email address. If the highlighted email address contains characters that aren't in the company's main website, it could be a fake email address.
- Avoid clicking on links in unsolicited emails and be wary of email attachments.
- Do not reveal user credentials, personal or financial information in an email or online.
- If you receive a suspicious email, report it via your company's reporting protocol or via spam@optum.com by forwarding the email as an attachment so originating information is included.

Resources

- For more information, please visit COVID-19 Resources Page
- For more Policy information:
    - Integrated employees, see our Security Policy and Standards on the Hub within eGRC.
    - Non-Integrated employees, see our Security Policy and Standards on the SAFE With Me Portal.