COVID-19: Working from Home Security and Privacy Reminders

March 27, 2020

During this global health crisis, many colleagues are working from home (also known as telecommuting), as permitted for their responsibilities and roles. There are a few important safety, privacy and security reminders for colleagues who are working remotely during this period. These are particularly important for colleagues with responsibility for handling our patient's protected health information (PHI) and other confidential information.

Below is a list of secure actions to take as you use MercyOne laptops and desktops in a remote environment:

1. **Work only from home** – Work only at home, not in other locations, for public safety reasons. If you do not have a dedicated home office, please find a private space to work in your home.

2. **Securely connect to the CommonSpirit or Trinity Health network** - ALWAYS set up a secure, virtual private network

3. **Establish a VPN connection** from your CommonSpirit or Trinity Health device after logging on. This establishes a secure connection to all Trinity Health network protections. See the [Remote Access Training Center](#).

4. **Protect your laptop or PC** - Keep your device in the house and stored in a laptop case during non-work hours. Shut down when you are finished for the day; don’t just turn off monitors. Lock the screen (control + alt + delete) when you walk away from your computer. Do not allow family members or other unauthorized individuals to use your laptop, desktop or mobile device. Even innocent behavior, as letting a teenager check their personal email, can introduce malware to the system and our network.

5. **Participate in phone calls/virtual meetings in private** – Use headsets or ear buds and use a private space away from other people in the home when discussing confidential information.

6. **Paper and printing** – Keep PHI and MercyOne business confidential information properly secured to prevent other individuals from viewing it. Do not discard your work product or any patient information in the trash. Instead, either shred the documents using a cross-hatch shredder or bring them back to the office. Do not print PHI on home printers.

7. **Delete data when no longer needed** – Remove or delete Confidential Data when it is no longer needed, including from the Windows recycle bin.

8. **Limit streaming services when working** – Avoid using streaming services like Netflix, Spotify and Pandora which may impact network performance while connected to the CommonSpirit or Trinity Health network. These services use significant network bandwidth, which may prevent colleagues from reaching critical resources.

9. **Do not change any device in any way** – Do not install unauthorized software packages on any device or make other changes like upgrade processor, expand memory or extra circuit boards. If additional memory or processing is needed, contact the IT Support Desk (CommonSpirit: 515-
643-3060; Trinity Health: 888.667.3003) for assistance. Do not install unauthorized software packages on any CommonSpirit or Trinity Health device.

10. **Report lost or stolen devices** – Trinity Colleagues should contact the TIS Service Desk immediately at 888.667.3003. CommonSpirit colleagues should contact CommonSpirit ITS Support Desk at 515-643-3060. Additionally, contact your supervisor or Privacy Official if you work with PHI.

11. **Be careful with email** – Be aware of malicious phishing messages on both work and your personal devices that try to take advantage of the COVID-19 pandemic. These messages contain coronavirus-related information such as security tips. There have been a high number of attacks leveraging COVID-19 to initiate a response. Report suspicious messages using the reporting button on your Outlook toolbar or forward the message as an attachment to:

   a. CommonSpirit colleagues: spam@catholichealth.net
   b. Trinity Health Colleagues: spam@trinity-health.org

For other security-related questions, please email your MercyOne Privacy Official or speak with your supervisor.

Thank you for continuing to be a Guardian and doing your part to keep our patient’s data secure during this unprecedented time.