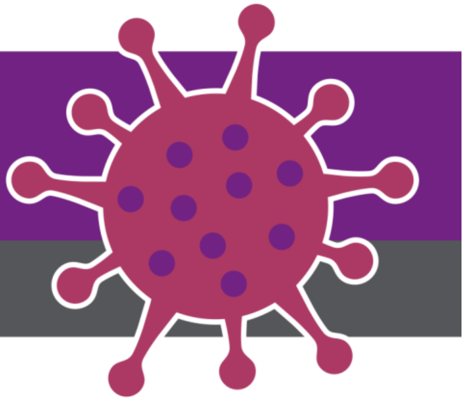
CORONA**VI**RUS **D**ISEASE 2019
(COVID-19)



Working from Home Security & Privacy Reminders

Trinity Health

Audience: All colleagues	
Revision Date: 3/24/2020	
Version: #1	

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 Trinity Health 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 Trinity Health network** - ALWAYS set up a secure, virtual private network (VPN) connection from your Trinity Health device after logging on via Connect portal, or an Aruba device if one was provided. This establishes a secure connection to all Trinity Health network protections. See the Remote Access Training Center.

3. **Protect your laptop or PC** - Keep your Trinity Health 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 Trinity Health 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.

4. **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.

5. **Paper & printing** – Keep PHI and Trinity Health business confidential information paper secured as much as possible to prevent other individuals from viewing it. Shred when no longer needed with supervisor permission. Do not print PHI on home printers.

6. **Delete data when no longer needed** – After receiving permission from your supervisor, remove or delete Confidential Data when it is no longer needed, including from the Windows recycle bin.

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

8. **Do not change any Trinity Health device in any way** – Do not install unauthorized software packages on any Trinity Health 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 for assistance. Do not install unauthorized software packages on any Trinity Health device.

9. **Report lost or stolen devices** – Contact the TIS Service Desk immediately at 888.667.3003. Additionally, contact your supervisor or Privacy Official if you work with PHI.

10. **Be careful with email** – Be aware of malicious phishing messages on both Trinity Health 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 spam@trinity-health.org.

This information is in Trinity Health Acceptable Use procedure. Additional information will be provided on how to protect confidential data when working remotely.

For other security-related questions, please email Ask Cybersecurity 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.