Maryland
DEPARTMENT OF HEALTH

Office of Enterprise Technology
MDH Pandemic Telework Resource Guide

This guide will assist you to answer these telework-related questions:

- What resources will I need to telework?
- What systems will I need to access as they telework?
- What computer and network resources will I need?
- How do I set up my home and work computer for teleworking?
- What forms will I need to read and sign to confirm my telework responsibilities, including how to keep MDH information, network, systems and computers safe while I work?
- Who can I call to get answers to telework questions?

The ongoing response to the Coronavirus (COVID-19) in Maryland will require some of us to work remotely. In order to contain the spread, the State has implemented Level II - Flexible Operations as outlined in the Pandemic Flu and Other Infectious Diseases Attendance and Leave Policy.

It is important to work with and communicate directly with your managers and supervisors to understand the expectations of teleworking and what you are expected to do away from the office.

This document also provides links to resources, forms, and support to help you telework successfully. We will also provide information to obtain remote access and where to go for support.

Maryland
DEPARTMENT OF HEALTH

Telework and Computer Use Agreements

We recommend, prior to teleworking, you read and sign the Interim Pandemic-Associated Teleworking Agreement, even if you have signed copy of the standard telework agreement on file. Employees are also required to follow the Maryland Computer Use Agreement which you signed when you were hired.

Security

Staff who have been issued laptops, tablets, or phones by MDH are less at risk in handling sensitive data, communications and private material than those who will telework using their personal devices. Teleworkers who use their own desktop or laptop PCs for telework should secure their operating systems and primary applications.

- Use a combination of security software, such as antivirus and antispyware software, personal firewalls, spam and Web content filtering, and popup blocking, to stop most attacks, particularly malware.
- Restrict who can use the PC by having a separate standard user account for each person, assigning a password to each user account, using the standard user accounts for daily use, and protecting user sessions from unauthorized physical access.
- Ensure that updates and patches are regularly applied to the operating system and primary applications, such as Web browsers, email clients, instant messaging clients, and security software. Click here for more cybersecurity related information.

You should also understand the security risks associated with taking paper away from the work site. Read this document to understand the do's and dont's.

You should also do a health check to ensure your work, MDH-supplied laptop/tablet or home computer security requirements. Click here to see how to do that.

Applications, Systems, and Data Access

When finalizing your telework needs, review this list of applications to determine if you need applications from Group 1 and/or Group 2. You will use this information to determine which solution you should use to identify the proper remote access solution i.e. VPN, Chrome, or Chrome Remote Desktop.

NO ONE SHOULD EVER TAKE THEIR WORK DESKTOP HOME.

If the work you do needs access to applications in Group 1, all you need is a home computer that has browser access. Caution: Some applications may work better in a specific browser - Chrome, Firefox, etc.

If the work you do needs access to applications in Group 2, (and Group 1), you have two options - VPN or Chrome RDP. In both cases your work desktop needs to be turned on.

Any employee that has a desktop at work and has either a state issued laptop or personal computer to use at home **does not currently need VPN to telework, and should use Chrome RDP**. New VPN requests will only be accepted for users who cannot access their work via Chrome RDP.

Option 1: VPN Soft Token

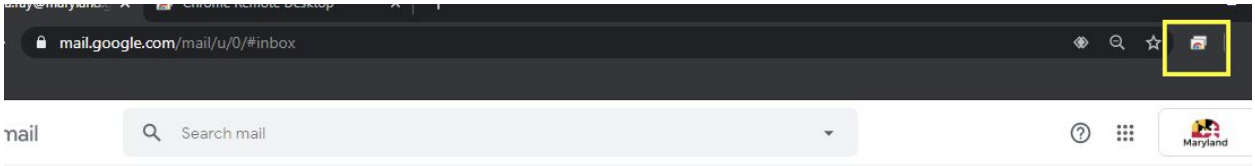
Some employees will need a VPN (Virtual Private Network) account if their work requires access to secured systems - MMIS, FMIS, Help Desk tracking and response tools, MD THINK portals, mapped network drive, etc. These are internal, secure systems that require verification that the user has the rights and privileges to access. Specific users will receive credentials (user name, password, authentication) to get access. Some will receive a token (likely a phone app), that would create specific user information and passwords to enter. Contact the help desk that supports your organization if a new VPN account needs to be set up to work remotely. This video shows how to install a soft token once you've received an account.

Important: If you have a Maryland provided laptop or tablet, you must set up your VPN account at the work site. It cannot be set up away from the office.

Option 2: Google RDP (Remote Desktop Protocol)

You can connect to a computer running Windows from another computer running Windows that's connected to the same network or to the Internet. This access would also require specific security protocol to ensure that the vulnerabilities of a home PC are not passed along to work systems and servers.

Chrome RDP is already loaded onto most MDH desktop computers (call local IT support if it is not). It's the icon highlighted by the yellow box in the upper right corner of your Chrome browser when signed into your Maryland account.



Step one is setting up your work computer. **Step two** is setting it up on your home computer. Click here to read the instructions, which will require you to create a PIN for your Chrome RDP account. Once you have it set up on your work and home computer you can log in to use it using the PIN you entered on your work computer.
IMPORTANT TIP: If your work computer has two monitors you will see images of both on your remote computer. At the left or right center, you will see an arrow in a blue semicircle. Click it and scroll down to the Display option and choose the one you want to work from. That will make your main work computer screen your work screen.

If you have an MDH-assigned laptop/tablet and no work desktop, and you need access to applications from Group 2 you need VPN.

Support:
If you are having computer issues working remotely, contact your local IT support first. If you do not have a local support team, contact **OET Support - 410 767-6534 or** mdh.oetsupport@maryland.gov.
You can also contact them through the website servicedesk.health.maryland.gov.

Telecommunications:
A business or personal cell phone, or a home phone can be used to conduct work remotely. If you do not have a MDH-issued cell phone, and do not want those you are calling, or those who are calling you, to see your number, there are a number of masking/second number solutions, e.g. Google Voice or the Burner app. If your home computer has Office 365, Skype is also an option to obtain a second number so you do not have to expose your personal number.

If someone has an MDH-issued phone and does not have internet access at home, they should get a personal Hotspot or Jetpack. Click here to fill out a request form.

Staff working from home should regularly check their work voice mail regularly. This document will guide you through the steps.