PHC Working Remotely Toolkit

Frequently Asked Questions

Who is eligible to work remotely?

Eligibility to work remotely is based on three criteria:

1. Where the employee's job is best performed
2. The employee's demonstrated performance
3. The suitability of the employee's remote work environment

Approval is determined on a case-by-case basis by an employee's manager, with the primary consideration being operational feasibility.

Working remotely is a privilege not a right; PHC may refuse to grant an employee's request to work remotely.

As a health care provider, most PHC employees provide direct patient care or other services that support care and therefore best perform their job on site; however, as PHC is a large and diverse employer there are employees for whom working remotely is an option.

Can I change my work hours if I am working remotely?

No. When working remotely, an employee's work responsibilities, work hours and eligibility for authorized overtime are not altered and they continue to be managed through existing policies and processes.

Compressed Work Weeks and Extended Work Days are not part of working remotely.

What about supervision and performance appraisal?

In a Working Remotely Agreement, an employee has the same performance accountabilities when working remotely as they do when working on-site. Similarly, a manager has the same supervisory accountabilities to employees working remotely and they do to employees working on-site.

Will PHC pay for the cost of setting up a home office and/or pay for a portion of home internet, heat and electricity for employees working from home?

Not at this time. PHC is offering working remotely as an option that can support our employees' work life balance, reduce their commuting time and costs, and reduce out of pocket expenses, like business clothes and eating out. Working remotely can improve the quality of life for our staff, particularly those with long commutes, young families or aging loved ones. According to a May 2020 survey of more than 600 PHC staff, our employees want the option to work remotely for a portion of their work time.

Will PHC issue a Form T2200 for tax purposes?

Our process for issuing a Form T2200 is under review. However, Canada Revenue Agency (CRA) will allow individuals working from home in 2020 due to COVID-19 to claim up to $400 in home office expenses without filling out any forms. CRA has also provided a Form T2200S for those people who believe their claim will be more than $400. For more information on claiming home office expenses, go to: canada.ca/cra-home-workspace-expenses.

Can employees take any of their PHC technology home?

If an employee has a PHC laptop, make sure the laptop has Citrix Gateway VPN installed so that the employee may use it when working remotely. Other than PHC-issued laptops, PHC is not supplying technology for employees to take home.

What about office supplies?

PHC will provide office supplies as needed. Out-of-pocket expenses for other supplies will not be reimbursed.

Privacy & Security

What are my obligations with respect to privacy and security?

Privacy and security are everyone's responsibility including when working remotely. The privacy and security controls present in the office are not always available at home or in public, so extra care is needed while handling work-related information off-site.

To learn more about our best practices for secure remote working, check out this infographic and learn about your security responsibilities.

How do I keep my computer secure?

Learning how to keep your computer secure starts with privacy and security awareness. Whether you are working on-site or remotely, please ensure you are aware of these common security threats, including phishing. If you think you have received spam or a phishing email, forward the email to spam@phsa.ca then delete the email from your Inbox folder and Deleted Items folder.

How do I keep my workspace secure?

To keep your workspace secure, please ensure you:

- Maintain a secure physical workspace.
- Close all work-related documents and applications when not working.
- Secure documents containing confidential and personal information in a locked drawer or cabinet.
- Log off your computer when not in use.
- Store USBs or hard drives in a locked cabinet or drawer when you are not present.

I may need to work in a public setting. Is it safe to use public Wi-Fi?

No. Hackers can intercept information travelling through public Wi-Fi. If using public Wi-Fi is absolutely necessary, use Citrix Gateway (VPN) as added security.

How do I keep my workspace secure in public?

If you must work remotely in public, remain vigilant and do not to leave your devices or documents unattended. Avoid using public Wi-Fi connections. Be wary of shoulder surfers and ensure your device's screen is not easily viewable by others. Place your computer in a secured bag when not in use and keep it with you at all times. To learn more, check out the Working Remotely - Cybersecurity Best Practices.

How do I ensure data is secure?

If working off-site, protect confidential information, by working with and keeping data on the Health Authority network and workstations where possible, using Citrix Remote Access or Citrix Gateway VPN.

How do I encrypt a USB key and hard drive?

If USB drives and hard drives are used to store documents that contain sensitive patient information, these drives must be encrypted. Refer to IMITS STANDARD #24: Mobile Storage Device Security Standard.

How do I securely share files?

Sharing files outside the Health Authority networks may increase the risk of information being exposed to unauthorized persons. Encrypting files is a method that helps secure data during transmission. To password-protect your document, workbook or presentation in Microsoft Word, Excel or PowerPoint, click File > Info > Protect Document. You can also password-protect your PDF.

Refer to sharing information outside the organization and the IMITS Secure File Sharing Standard.
Refer to PHC Email Policy before sharing personal information through email.

Is it necessary to have strong passwords on the personal devices I plan to use for work?

Yes. A strong password provides essential protection from data theft. Hackers often break into computers by guessing passwords. Consider using passphrases where applicable.

What do I do if my work device is lost or stolen?

Report it to the Service Desk immediately. Email servicedesk@vch.ca or phone 604.806.9333.

Where can I get more information about how to work remotely?

Email IMITSSecurity@phsa.ca with questions or concerns or visit the IMITS Infocentre.

Remote access

What type of remote access do I need?

There are several different remote access options available for staff to work from home. Staff can access PHC systems and applications from a personal computer or a PHC-issued laptop. Click here to review the various options.

How do I access the health organization network off-site from my personal computer?

To access the health organization network from a personal computer, you will need to use Citrix Remote Access – see details under Internal Websites, Network Drives/Files & Microsoft Office. You will also need to register for a Microsoft Authenticator Remote Access token if you do not have one already.

What are the benefits of using the Citrix Remote Access?

Citrix Remote Access allows you to use a personal computer to access a variety of internal applications, the health organization network and the ability to control a specific workstation remotely. When using Citrix Remote Access, all data and files remain on the health organization network and are not stored on the personal computer.

How do I access the health organization network off-site from my PHC laptop?

Use Citrix Gateway VPN to connect to the health organization network directly from your PHC laptop as if you were at work.

See the Remote Access guide for details. You will also need to register for a Microsoft Authenticator Remote Access token if you do not have one already.

What are the benefits of using the Citrix Gateway VPN?

Citrix Gateway VPN allows you to access intranets (e.g., PHC Connect, PeopleSoft, etc.), shared drives/folders and internal applications, similar to working on site. You can also change your network password and allow your laptop to receive updates.

Is the Citrix Gateway VPN an upgraded version of Citrix remote access?

No. While the current Citrix connection does allow remote access to your health organization network, there are critical tasks that cannot be done without the Citrix Gateway VPN. For example, warning messages and password mismatches between laptop and domain can only be remediated (remotely) once the Citrix Gateway VPN is installed.

Can I install the Citrix Gateway VPN on my personal laptop?

No. The Citrix Gateway VPN software cannot be installed on personal devices or non-PHC issued laptops. Personal computers should use Citrix Remote Access instead.

Who do I contact for help with Remote Access?

Contact the IMITS Service Desk at servicedesk@vch.ca or phone 604.806.9333 for assistance or to report an issue.

For more information and resources, visit the IMITS InfoCentre, a central source of IMITS information and services.