1. Purpose

The purpose of this document is to outline the terms and conditions for a Teleworking/Working from Home Program for Providence Health Care (PHC) for the duration of the COVID 19 pandemic. These reflect the intent of PHC to provide flexibility for both the employer and the participating employees by offering employees the opportunity for Teleworking. It is understood that if the situation changes that the employee might be required to physically come back to their workplace.

2. Overview

Teleworking enables an Employee to work from home for extraordinary purposes, such as the COVID19 pandemic. It does not change the nature of the work that an Employee is expected to perform or the hours an Employee is expected to work. These guidelines set out the expectations and requirements associated with Teleworking.

3. Guiding Principles for Teleworking

The employer and employee shall consider the following guiding principles for Teleworking/working from home:

- The total hours worked by an employee will not change.
- Employees must be performing satisfactorily and maintain their performance.

4. Working Alone Call-in Procedures

When employees and their managers do not work in the same location, managers remain responsible for ensuring that their employees are at work and all is well. Working alone call-in procedures, via email, text or phone, should be established by the responsible manager.

5. Information Privacy and Security

Patient/client/resident confidentiality is a large consideration when arranging an at-home workspace to ensure no other person in the household can view information. Employees are responsible for protecting the security and privacy of the information they handle and the technology they use. Employees must be aware of and comply to all applicable policies including PHC's Information Privacy and Confidentiality Policy as well as Managing Privacy Breaches Policy.

6. Technical and Physical Assessment

The checklists below will help managers determine if their employees have a home working environment that provides the security and privacy for carrying out their role. If managers are not sure, they should contact the Information Access & Privacy Office.

7. Technical & Physical Assessment – please complete this checklist

Category				
Part 1 – Technical Assessment	**Yes**	**No**	**Don't Know**	**Comments**
Work issued Computer				
1. Will you be using a computer provided by the Employer?				If YES, skip to number 17.
General – Home Computer				
2. Will you be using your personal computer?				
3. Will you be accessing files and doing your work through remote access (Citrix) to your network drives (using VPN/MobilePASS)?				
4. Will you be accessing Outlook via webmail.				
5. Will your work involve emailing documents containing patient/client/resident/Staff or other personal information?				
Home computer – other users				
6. Is there more than one user of the home computer?				
7. If you are using a shared home computer, is there a separate user profile and access password set up for your work-related activities only?				
8. Is the screen saver set to time out after no more than 15 minutes of inactivity?				
9. Does the screen saver require a password for re-activation?				
Home computer – Virus Protection / Firewall				
10. Is there active anti-virus software installed on the computer? E.g. Norton, Bitdefender, Kaspersky				
11. Is the anti-virus software configured to receive updates regularly?				
12. Is a full computer virus scan set to run on a weekly basis?				

Home computer – Operating System, Internet browser, Application Software	Yes	No	Don't Know	Comments
13. Is the Operating System (OS) up-to-date (Windows update, Mac OS updates)?				
14. Are you using locally installed, stand-alone office applications to **work on confidential and/or personal information**? E.g. Microsoft Office				
15. Are the applications (e.g. Microsoft Office, Adobe Reader) kept up-to-date with security patches?				
Home computer - Other				
16. Will confidential and/or personal information be stored on your home computers hard drive? **If yes, please contact the PHC Privacy Office.**				
17. Is confidential and/or personal information being stored on an encrypted device (e.g. Employer issued encrypted USB flash drive)?				
18. Does your home wireless network have a secure password?				
19. Does your home wireless network have encryption enabled?[1]				
Part 2 – Physical Assessment				
20. Will you be required to transport confidential documents in paper or electronic format (e.g. on a USB) between a PHC site and your home? 21. If yes, please provide details.				
22. Are computer monitors positioned so that unauthorized individuals cannot see the screen?				
23. Will you be required to print documents containing personal or confidential information?				

[1] To find out if your wireless network has encryption enabled you can:

- Google the model number of your router and look for the manual online
- Call your Internet Service Provider (e.g. Telus, Shaw) for support

Part 2 – Physical Assessment, continued	**Yes**	**No**	**Don't Know**	**Comments**
24. Is there a secure storage area (e.g., lockable drawer, box, room) to protect devices and/or paper containing confidential and/or personal information?				
25. Are paper copies of confidential and/or personal information disposed of securely? Explain.				
26. Will you have conversations with or about patients/residents/clients via phone or videoconferencing?				
27. Do you have a private space in your home to have those conversations?				

Part 3	
Form completed by: _____ Employee Signature	Date: _____
Information verified by: _____ Manager / Leader Signature	Date: _____

8. Other Resources

- IMITS Infocentre – "Secure Computing": http://imitsinfocentre.healthbc.org/secure-computing
- IMITS Infocentre – "Working Remotely - Cybersecurity Best Practices": http://imitsinfocentre.healthbc.org/secure-computing/remoteaccess-faq
- IMITS Infocentre – "Coronavirus Phishing Emails": http://imitsinfocentre.healthbc.org/covid19-scams