**Privacy and confidentiality for researchers working from home**

To respond to COVID-19 pandemic, many researchers are now needing to work from home and therefore, may need to adapt their project. This document will provide some guidance to working from home.

**Change to your research project?**

Please ensure that any changes to your research project as a result of changing to your work location, have been approved by the REB through a formal amendment.

**Is your work environment suitable?**

If you are working from home or from another remote location, you must review and complete the checklist that is appended to this document[: ***Guidelines for Teleworking/Working from Home - Interim guidelines to respond to COVID-19***](#_Purpose)*.* Once completed it must be reviewed by the Principal Investigator to ensure the appropriate privacy and security controls are in place for you to be conducting your research activities. This checklist will help to assess whether you have the appropriate controls for your computer, and also a private environment within which to work. Once the form is completed and reviewed, it should be stored by the Principal Investigator.

**Other Considerations**

**Recruitment:**

* Recruit participants by phone, email, or through an approved videoconference tool.

**Consent Options**:

* Consent participants remotely through the [UBC](https://arc.ubc.ca/redcap) or [CHEOS](http://www.cheori.org/en/REDCap) instance of REDCap , or through the [BCAHSN](https://redcap.bcahsn.ca/). When you amend your application in RISe, add the following statement to the consent form “Your electronic consent form will be stored in the XXXXX secured network in Vancouver, BC. Only authorized personnel will be able to access it.”
* Consent participants verbally by phone or through a virtual health tool. Document verbal consent in the participant’s research file.

**Data Collection:**

* Access participant electronic medical records through [PHC Remote Access](http://imitsinfocentre.healthbc.org/services/remote-access-tokens) – Citrix, if eligible.
* Perform interviews or follow-up activities with participant by phone, email, or video conference.

**Data Analysis**:

* Access files through [PHC Citrix](https://remoteapps.healthbc.org/logon/LogonPoint/tmindex.html) or [UBC VPN](https://it.ubc.ca/services/email-voice-internet/myvpn).
* De-identify datasets for data analysis purposes.
* Transfer sensitive data between team members by using [IMITS Secure File Transfer Service](http://imitsinfocentre.healthbc.org/services/secure-file-transfer) or [UBC Workspace 2.0](https://it.ubc.ca/services/web-servers-storage/workspace-20)
* Store research data, if required, on an encrypted USB or a hard drive encrypted laptop.
* Delete all data upon completion.

**Email:**

* Use an institutional email address to communicate with participants and with your research team.
* Review and comply with PHC [Email Policy](http://www.providencehealthcare.org/sites/default/files/CPN0500%20Emailing%20Policy%20FINAL%20%28August%202017%29%20SLT%20August%2030.pdf)  and [Guidelines](http://toolkit.providencehealthcare.org/sites/toolkit.providencehealthcare.org/files/EmailGuidelines.pdf) .
* Provide participant with [PHC Emailing Notice to patients](http://www.providencehealthcare.org/sites/default/files/VCH%20PHC%20Emailing%20or%20Texting%20Notice%20%2817%20Jul%2026%29.pdf).
* Ensure that files are password protected and the passwords to those files are sent in a different manner (e.g. by phone, text).
* Never transfer identifiable information via email unless this has been pre-approved by the REB.

**Virtual Health / Videoconferencing Tools:**

* Follow [PHC Virtual Health Guidelines](http://covid19.providencehealthcare.org/information-medical-staff/qa-medical-staff/virtual-health) for tools such as Skype for Business, FaceTime, or Zoom. Note, that only license version of Zoom is approved, request license at <https://surveys.divisionsbc.ca/ZoomAccount.survey>).

**Other tips**

* Ensure any changes to how you communicate with participants is reflected in an amendment in RISe and approved by REB.
* Restrict the copying of research data. The more copies you have, the increased risk of a privacy breach. Destroy/delete any copies of data as early as possible.
* Be especially careful with identifiable information. Identifiable data should never leave Providence Health Care or another Health Authority environment unless approved in advance by the REB.
* Keep track of where all your data is stored, including any copies.

**For more Information:**

* PHC has designated page with guidelines and Q&A for Researchers that address COVID concerns at <http://covid19.providencehealthcare.org/information-researchers>
* The UBC Research Ethics Office recently posted a series of FAQs that address some of the key concerns relating to the continuity of research activities including questions about research funding and fieldwork. It can be found here: <https://research.ubc.ca/research-faqs-relating-covid-19>

**You can also contact the PHC REB or Privacy Office:**

Julie Hadden

Manager, Ethical Reviews - Policies, Standards, REB Administration

julie.hadden@ubc.ca

PHC Information Access and Privacy Office

privacy@providencehealth.bc.ca

**Appendix A: PHC Working from Home Checklist**

# 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.

# 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.

# 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.

# 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.

# 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](http://shop.healthcarebc.ca/phc/PHCPolicies/B-00-11-10108.pdf) as well as [Managing Privacy Breaches Policy.](http://shop.healthcarebc.ca/phc/PHCPolicies/B-00-11-10120.pdf)

# 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.

# 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** |  |  |  |  |
| 1. Will you be using your personal computer?
 |  |  |  |  |
| 1. Will you be accessing files and doing your work through remote access (Citrix) to your network drives (using VPN/MobilePASS)?
 |  |  |  |  |
| 1. Will you be accessing Outlook via webmail.
 |  |  |  |  |
| 1. Will your work involve emailing documents containing patient/client/resident/Staff or other personal information?
 |  |  |  |  |
| **Home computer – other users** |  |  |  |  |
| 1. Is there more than one user of the home computer?
 |  |  |  |  |
| 1. 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?
 |  |  |  |  |
| 1. Is the screen saver set to time out after no more than 15 minutes of inactivity?
 |  |  |  |  |
| 1. Does the screen saver require a password for re‐activation?
 |  |  |  |  |
| **Home computer – Virus Protection / Firewall** |  |  |  |  |
| 1. Is there active anti‐virus software installed on the computer? E.g. Norton, Bitdefender, Kaspersky
 |  |  |  |  |
| 1. Is the anti‐virus software configured to receive updates regularly?
 |  |  |  |  |
| 1. 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** |
| 1. Is the Operating System (OS) up‐to‐date (Windows update, Mac OS updates)?
 |  |  |  |  |
| 1. Are you using locally installed, stand- alone office applications to **work on confidential and/or personal information**? E.g. Microsoft Office
 |  |  |  |  |
| 1. Are the applications (e.g. Microsoft Office, Adobe Reader) kept up‐to‐date with security patches?
 |  |  |  |  |
| **Home computer - Other** |  |  |  |  |
| 1. Will confidential and/or personal information be stored on your home computers hard drive? **If yes, please contact the PHC Privacy Office.**
 |  |  |  |  |
| 1. Is confidential and/or personal information being stored on an encrypted device (e.g. Employer issued encrypted USB flash drive)?
 |  |  |  |  |
| 1. Does your home wireless network have a secure password?
 |  |  |  |  |
| 1. Does your home wireless network have encryption enabled?[[1]](#footnote-1)
 |  |  |  |  |
| **Part 2 – Physical Assessment** |  |  |  |  |
| 1. 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?
2. If yes, please provide details.
 |  |  |  |  |
| 1. Are computer monitors positioned so that unauthorized individuals cannot see the screen?
 |  |  |  |  |
| 1. Will you be required to print documents containing personal or confidential information?
 |  |  |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Part 2 – Physical Assessment,** continued | **Yes** | **No** | **Don’t Know** | **Comments** |
| 1. Is there a secure storage area (e.g., lockable drawer, box, room) to protect devices and/or paper containing confidential and/or personal information?
 |  |  |  |  |
| 1. Are paper copies of confidential and/or personal information disposed of securely? Explain.
 |  |  |  |  |
| 1. Will you have conversations with or about patients/residents/clients via phone or videoconferencing?
 |  |  |  |  |
| 1. 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: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |

# Other Resources

* IMITS Info Centre – “Secure Computing”: <http://imitsinfocentre.healthbc.org/secure-computing>
* IMITS Info entre – “Working Remotely - Cybersecurity Best Practices”:  <http://imitsinfocentre.healthbc.org/secure-computing/remoteaccess-faq>
* IMITS Info Centre – “Coronavirus Phishing Emails”: <http://imitsinfocentre.healthbc.org/covid19-scams>.
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 [↑](#footnote-ref-1)