Privacy and confidentiality guidance for researchers working from home

From working in the office to working from home, we are here to support you. If you need help from VCHRI, please send us an email and we will reply as soon as we can. The contact information is at the end of this guidance.

Security at home

- Position your home computer screen away from prying eyes.
- Password protect your home computer.
- Password protect any sensitive files.
- Lock your device before stepping away.
- Install an antivirus software (e.g. Sophos free antivirus software).
- Avoid connecting devices to public Wi-Fi as it lacks strong security controls

Email

- Use institutional email address and never use personal email accounts (e.g. Gmail, Hotmail, Yahoo, etc.) for research related tasks. Never transfer identifiable information via email unless this has been pre-approved by REB and VCHRI. Follow UBC's Information Security Standard #03 and Encryption Requirements standard, as well as VCH's Emailing Policy and Guidelines.
- Ensure files are password protected and the passwords to those files are sent in a different manner (e.g. by phone, text).
- Before sending an email, ensure it is to the correct recipient.
- Watch for phishing emails. Do not click on any links or attachments within the email. Forward email to spam@phsa.ca immediately and delete the email from the inbox, sent items and deleted items folder.

Security of Research Data and Information

- Work in secure virtual private network (remote access), depending on your appointment, be sure to follow the UBC Information Security Standard #06 or the health authority's IMITs Remote Access procedures. If full remote access is not required on the health authority's platform, use the IMITs virtual desktop.
    - UBC myVPN
    - IMITs Remote Access (oneVCH intranet)
    - Non VCH employee (external researcher), contact Research Privacy Advisor.
- Limit the transfer of identifiable information only when it is absolutely necessary and limit the number of team members who can view it and use it. Identifiable data should never leave the Health Authority environment unless this has been approved in advance by the REB and VCHRI. Keep track of where all your data are including copies.
- Transfer sensitive or share confidential data between team members using Secure File Transfer Services (sftp). Files containing private/confidential information must be sent with appropriate security measures using passwords or encryption. Passwords should be provided in a different manner (e.g. by phone, text). Please also ensure that recipients secure the information appropriately.
    - UBC Computing Services FTP (Other ways to stay secure: privacymatters.ubc.ca)
    - IMITS Secure File Transfer Service via oneVCH intranet (Remote Access Policy)
- Encrypt and password protect portable storage devices (USBs, hard drive, etc.)
- Limit the amount of copies you have of research data. The more copies you have, the more you increase the chance of a breach.
    - Extra copies of data should be destroyed or deleted as early as possible.

- When paper copies are not being used, store in a secured location such as a locked filing cabinet or desk drawer.
- Do not transport documents that contain participant personal information or original health records to your home.

Mobile devices

- Password protect your device
- Lock your device when not in use
- Keep your software up-to-date

Virtual Tool:

- Consider communicating with participants remotely when possible.
- VCH virtual tool **Zoom** may be used for video conferencing with patients and research participants. Follow *Best Practices* and *User Guides* for securing your meetings. When requesting license (oneVCH intranet), select 'Admin' under heading called User Type.
- Ensure any changes to how you communicate with participants are reflected in an amendment and approved by REB. See the UBC REB guidance and sample template consent form addendum.

Breach

- Report any breach of personal information to the Research Privacy Advisor immediately, whether accidentally or intentionally. Follow VCH policy on Reporting and Management of Information Privacy Breaches.

Additional information:

- *Working from home? Follow these best practices*: https://my.vch.ca/news-discussion/secure-remote-work
- *5 steps to secure your mobile device*: https://my.vch.ca/news-discussion/mobile-security
- *Working remotely:* https://my.vch.ca/covid19/working-remotely
- *COVID-19: Curtailing Research Activities on UBC Campuses:* https://research.ubc.ca/covid-19-curtailing-research-activities-ubc-campuses
- *VCHRI COVID-19 Information and FAQs:* https://www.vchri.ca/covid-19-information-and-faqs
- *Tips for public bodies and organizations setting up remote workspaces:* https://www.oipc.bc.ca/guidance-documents/2398
- *Top 15 Tips. Mobile Devices: Tips for Security & Privacy:* https://www.oipc.bc.ca/guidance-documents/1994.

Questions?

Contact: Anna Low
Research Privacy Advisor
Vancouver Coastal Health Research Institute | Data Release Management Office
Email: anna.low@vch.ca
Website: www.vchri.ca