Vancouver CoastalHealth
Promoting wellness. Ensuring care.

We all play a part … … be privacy and security smart!

We all play a part…

Regardless of our roles and affiliations, best practice for keeping data safe is to limit the collection of personal information, de-identify data as soon as practicably possible, and handle data in a secure and respectful manner.

…be privacy and security smart!

Encrypt to Secure

Encryption is the first step in protecting data. Encryption is the process of encoding data in such a way that only authorized parties can access it.

Secure information by using:

- Encrypted USB devices[i]
- Encrypted documents (WORD, EXCEL, PDF) [ii]
- Encrypted hard drives (desktop or laptop computers and mobile devices) [iii]
- Encrypted transmissions (such as IMITS' **Secure File Transfer Service** for sharing of documents and files with VCH/PHC/PHSA staff) [iv]

Privacy Best Practices:

- Collect only the Personal Information you need to know to do the job at hand;
- De-identify data at the earliest possible time, unless the participant has consented to remain identifiable;
- Ensure all devices used for research are encrypted;
- Use strong passwords and keep them secret;
- Seek to store data on secure networks;
- Limit access to only those authorized to handle that information *and* who need the information to carry out the job as part of the research team.
- Store Personal Information Canada, unless participants have consented or where otherwise authorized by the REB and VCH.
- Know your obligations when doing research at VCH by reviewing the ***VCH & PHC Research and Data Access Terms and Conditions*** and ensuring all members of the research team sign the online ***VCH/PHC Confidentiality Undertaking for Researchers***;
- If you suspect a breach of VCH data has occurred, report it immediately to **privacy@vch.ca**.

Take the new online VCH/PHC Privacy and Confidentiality Undertaking! Complete your online Confidentiality Undertaking for Researchers between July 1st and July 31th, 2018 to be eligible to win one of eight $25 gift cards.

[i] See:

- UBC Information Security Guideline, How to Encrypt USB Sticks & Other Removable Media, online **https://cio.ubc.ca/sites/cio.ubc.ca/files/documents/resources/How%20to%20encrypt%20USB%20sticks%20and%20other%20removable%20media%20Guideline.pdf**

- How do I encrypt a USB Key and Hard Drive? On the IMITS InfoCentre (VCH/PHC/PHSA Intranet) **http://imitsinfocentre.healthbc.org/resources/how-do-i/security-and-access**

[ii] See:

- UBC Information Security Guideline, How to Encrypt Files Using Common Applications, online: **https://cio.ubc.ca/sites/cio.ubc.ca/files/documents/resources/How%20to%20Encrypt%20Files%20using%20Common%20Applications%20Guideline.pdf**

- IMITS Standard #12: Secure File Sharing Standard, on the IMITS InfoCentre (VCH/PHC/PHSA Intranet): **http://imitsinfocentre.healthbc.org/secure-computing-site/security-policies-standards-guidelines-site/Documents/IMITS-12-Secure%20File%20Sharing%20Standard%200.1_Apr2017.pdf**

[iii] See:

- UBC Information Security Guideline, Encrypting Mobile Devices, online: **https://cio.ubc.ca/sites/cio.ubc.ca/files/documents/resources/Encrypting%20Mobile%20Devices%20Guideline.pdf**

[iv] See:

- Secure File Transfer Protocol on the IMITS InfoCentre (VCH/PHC/PHSA Intranet): **http://imitsinfocentre.healthbc.org/services/secure-file-transfer**

- For UBC Affiliated Researchers (non-Health Authority Staff), consider using **Workspace 2.0**. Visit UBC Information Technology online: **https://it.ubc.ca/services/web-servers-storage/workspace-20**