QUICK REFERENCE GUIDE FOR PHC/PHCRI RESEARCHERS

Introduction

This document will provide researchers with quick and easy to find options and best practices to better protect the Personal Information (PI) of participants. These guidelines have been developed from researchers frequently asked questions and combines best practices from both Providence Health Care (PHC) and the University of British Columbia (UBC). Due to the evolving nature of technology, it is recommended that you check with your Privacy Office and IT department for updates to these guidelines.

The options provided within this document are based on privacy and security best practices and should be referenced when completing your REB application. Remember to be transparent in your application and fully describe how personal information will be handled and include information on any apps/devices/tools that will be used for your study.

If you have any questions about these guidelines, contact PHC IAPO by email at privacy@providencehealth.bc.ca.

This document covers:

Definition of Personal Information

FIPPA defines personal information as "**recorded information about an identifiable individual other than business contact information**" and includes any information that can be linked back to or identify an individual through reference or association.

Personal information may be a single personal identifier or element of information about you. While some information may not be considered identifiable personal information on its own, it may become personal information if there is a possibility that it could identify you when combined with other publicly available information.

Personal information may include, but is not limited to:

- Name, sex, date of birth
- Location - geographic subdivisions smaller than province including street address, city, country, postal code
- Elements of date (except year) related to an individual, including admit/discharge dates, surgery date, date of death, all ages over 89 years
- Telephone, fax, email
- Religious belief
- Social Insurance Number (SIN), Medical Record Number (MRN), Personal Health Number (PHN)
- Employee number, College ID
- Medical condition
- Device identifiers
- IP addresses
- Biometric identifiers (finger prints, voice and video recordings)
- Biological materials (tissues samples, blood samples)

Data Storage

Research data in both paper and electronic forms must be securely stored.

Paper Files

Paper records with participant personal information must be stored in locked file cabinets, desks, or closets within a locked office. UBC provides additional guidelines for securing paper records: https://rmo.sites.olt.ubc.ca/files/2021/04/PaperRecordsSecurity_GUI_0013_Rev1-1.pdf

Electronic Files:

Electronic files with participant personal information must be stored within organization or institution networks, behind firewalls and/or within UBC approved databases such as REDCap, MS OneDrive, etc. Data should only be accessed by approved members of the research team.

Electronic Devices:

Electronic devices containing participant personal information must be secured by physical and technical controls. Physical controls may include, but not limited to, using cable locks to secure desktop PCs and laptops to secure anchor points, , and storing mobile devices (such as USB Keys) in a locked desk within a locked office. Technical controls should include device and file encryption (see Encryption section).

Data Transfer

Research files containing personal information must be protected during the data transfer process. Below are some guidelines on how to securely share data using secure file transfer and email.

Secure File Transfer Service:
Transferring files using the IMITS Secure File Transfer Service for VCH, PHC, and PHSA http://imitsinfocentre.healthbc.org/services/secure-file-transfer or using a UBC approved tool such as Microsoft OneDrive https://arc.ubc.ca/microsoft-onedrive-and-teams-research are the most secure options for transferring data.

Email:
Emailing personal information or sensitive information is not recommended as a first option. However, in cases where emailing is the only available option, follow your organization's emailing policies and procedures.

- PHC: Emailing Policy - http://shop.healthcarebc.ca/PHCVCHPolicies/BD-00-11-40000.pdf
- UBC: How to Send Sensitive Information Over Email - https://isit.arts.ubc.ca/send-files-securely/

If you are unable to use a secure file transfer service or if email is not a suitable method for transferring your data, consult with your organization's privacy office or IT department for other transfer data options.

Encryption

Encryption is the scrambling of data so that only the authorized person (the password holder) can read it. Use AES-256 bit encryption for USB keys, hard drives, research Masterfiles, and mobile devices. Where AES-256 is not available, AES-128 bit is the next best alternative.

USB Keys (also referred to as Mobile USB Sticks or USB Drives):
Approved mobile USB keys can be ordered from your organization's Service Catalogue. Below are examples of USB keys that meet AES-256 bit encryption requirements and are FIPS 140-2 compliant (https://en.wikipedia.org/wiki/FIPS_140-2).

- Kingston DataTraveler 4000G2 or DataTraveler Vault Privacy Edition
- Kingston IronKey D300 or S1000
- Kanguru Defender Elite300
- Imation Powered by IronKey (Personal, Basic or Enterprise versions)

Check with your IT department if you require additional USB key recommendations or to check if a certain USB key model meets encryption standards.

File Encryption:
When it is necessary to encrypt a document for storing or sending to another individual (e.g. sending file by email), the following options are available:

- Microsoft Office (2007 or later for Windows, 2008 only for Mac) to encrypt Word, Excel & other MS Office files
- Adobe Acrobat for encrypting PDF documents
- 7-Zip (9.2.0), AES Crypt (3.08), or WinZip to encrypt files

Other Devices:
If devices such as desktop PCs and mobile devices (laptops, tablets, external hard drives, and smartphones) are used to store personal information, these devices must have encryption enabled. Since encryption capabilities and settings of each device and operating system (OS) varies by manufacturer, it is recommended that you check with your IT department and/or the device/OS manufacturer's website to confirm if encryption is enabled on your device or for instructions on how to enable it.

Additional Encryption Related Resources:

- UBC Encryption Requirement Standard
- UBC File Encryption Guidelines
- UBC – How to encrypt USB sticks

Retention

The following guidelines should be used when storing data associated with non-Health Canada clinical trials and Health Canada clinical trials, respectively:

- UBC initiated studies have to be retained at least for 5 years upon study completion based on to section 2.1.4 of UBC Scholarly Integrity Policy https://universitycounsel.ubc.ca/files/2022/05/Scholarly-Integrity-Policy_SC6.pdf; and
- As of February 11, 2022 retention period for Health Canada trials has been reduced from 25 years to 15 years. This information can be found at https://www.canada.ca/en/health-canada/services/clinical-trials/notice-period-reduced-keeping-records-drugs-natural-health-products.html .

Working Remotely

When working remotely, ensure personal information is handled and protected appropriately. If personal information is being accessed, you must use the organization's approved secure remote access tools (e.g. remote desktop, VPN, organization issued device, etc.).

Refer to the PHC and/or UBC Remote Work requirements:

- PHC: Working Remotely Toolkit - https://connect.phcnet.ca/life-career/employee-resources/working-remotely/
- UBC: Remote work at UBC - https://hr.ubc.ca/remote-work-ubc

Managing Privacy Breaches

Privacy Breaches occur when personal information has been lost, stolen or disclosed without authorization, whether accidentally or intentionally. An example of a privacy breach is when source documents are shared with the Sponsor without removing all of the personal identifiers such as name, DOB, PHN, MRN, diagnosis, or address. Other examples include when a laptop with research data is lost or stolen, or when patient information is accessed for reasons other than as authorized in the research application, such as accessing a medical record of a family member or friend.

Both PHC and UBC provides guidance for managing privacy breaches.

- PHC Managing Privacy Breaches Policy: http://shop.healthcarebc.ca/phc/PHCPolicies/B-00-11-10120.pdf
- UBC Report an incident: https://privacymatters.ubc.ca/report-incident

Where you have confirmed or suspect a privacy breach has occurred:

- Immediately notify your Principal Investigator;
- Notify the Research Ethics Board and the PHC Privacy Office;
- Take steps to contain the privacy breach.

Useful Links

Privacy Module and Confidentiality Acknowledgements:

- VCH & PHC Confidentiality Undertaking for Researchers: https://learninghub.phsa.ca/Courses/17110/vch-phc-confidentiality-undertaking-for-researchers
- Confidentiality Acknowledgement For Remote Monitors (look under Privacy Heading): https://www.providenceresearch.ca/research-ethics/resources#:~:text=Confidentiality%20Acknowledgement%20For%20Remote%20Monitors
  - Under Privacy Heading

Institutional Approvals:

- Providence Research Instructional Approval page: https://www.providenceresearch.ca/research-ethics/institutional-approvals
- Providence Health Care Hospital Approval Contacts: https://www.providenceresearch.ca/sites/default/files/PHC%20Hospital%20Approval%20Contact%20-%20March%202022.pdf
- Approval Form: https://www.providenceresearch.ca/sites/default/files/PHC%20Program%20Utilization%20Form%202021_2.pdf

Other Tools Available to Researchers

There are a number of tools available through the UBC Faculty of Medicine that can be used for App development, visualization, database development, or biobanking. More information can be found at https://mednet.med.ubc.ca/ServicesAndResources/IT/Research/Pages/default.aspx.