PHS HealthCare Privacy Policy

PHS HealthCare Privacy Officer: Dr. Christy Sutherland, Medical Director

Contact:
604-879-7906
350 Columbia Street
Vancouver, BC
V6A 4J1

Introduction

PHS HealthCare operates within PHS Community Services Society. BC's Personal Information Protection Act (PIPA) sets out rules for how organizations collect, use and disclose personal information. This act applies to the information that PHS HealthCare collects about the patients for whom we provide care.

As a team, we foster a culture of privacy, and work in compliance with PIPPA. PHS HealthCare and PHS Community Services Society is committed to being accountable for how we handle personal information, as well as how we follow the rules and procedures outlined in this policy.

Purpose

The purpose of this document is to outline PHS HealthCare Privacy Policy. It is to inform staff and patients about the privacy safeties we have in place, as well as to support staff to meet and adhere to privacy requirements.

The policy is available on our PHS staff intranet, on our website, and patients or the public will be provided a paper copy upon request.

What type of information we are collecting:

As per PIPA, personal information means information about an identifiable individual.

Contact information: name, email, phone, address, gender
Personal Health Number
Medical History such as symptoms, clinical conditions, medications, test results or allergies

We will collect only the minimum amount of data required to provide safe clinical care.

Who are we collecting personal information from?

People who present to PHS clinics requesting to become a patient of PHS HealthCare and are requesting medical care.

What is the purpose of collecting the information?

Medical care

Sensitivity of collected information

High sensitivity

How personal information will be used

The information used will only be used for the purpose of clinical care.

Consent to collect information

By virtue of seeking care from us, consent is implied (assumed) for personal information to be used by our clinic to provide care, and to be shared with other providers involved in care.

Consent can be withdrawn at any time. If someone wishes to withdraw consent, we will inform the person that we would no longer be able to safely provide clinical care.

We will only collect the information that is required to provide care, administrate the care that is provided, and communicate with patients.

PHS HealthCare will not collect, or use personal information other than for the purposes of medical care. In circumstances such as research, where information is requested from an external party, we will obtain additional consent from each individual.

PHS HealthCare will only disclose personal information where authorized by PIPA or required by law (for example, in the event of a court order, subpoena, or search warrant).

Disclosing information

Disclosure to other health care providers:

A person's implied consent extends to PHS HealthCare sharing personal information with other providers involved in a person's care, including (but not limited to) other physicians and specialists, pharmacists, lab technicians, nutritionists, physiotherapists, nurses and occupational therapists.

PHS HealthCare will only disclose personal information where authorized by PIPA or required by law (for example, in the event of a court order, subpoena, or search warrant).

Disclosures authorized by law:

There are limited situations where we are legally required to disclose personal information without your consent. These situations include (but are not limited to) billing MSP, provincial health plans, reporting infectious diseases and fitness to drive, or by court order.

Express consent from each person is required before we will disclose information to third parties for any purpose other than to provide care or unless we are authorized to do so by law. Examples of disclosures to other parties requiring express consent include (but are not limited to) third parties who are conducting medical examinations for purposes not related to the provision of care, enrolment in clinical (research) trials and provision of charts or chart summaries to insurance companies.

PHS Community Services Society has custody of the medical records.

Where we document personal information

All information is documented and stored on our electronic medical record, OSCAR. OSCAR is double password protected, and stored on a secure, Canadian based cloud.

Patient Rights

How can records be accessed?

Patients have the right to access their record in a timely manner. People may request a copy of their record, for a minimal fee. If they wish to view the original record, one of our staff must be present to maintain the integrity of the record, and a minimal fee may be charged for this access. Patient requests for access to a medical record can be made verbally or in writing to your physician or the staff (see office address at the top of our Privacy Policy).

Are there limitations on access?

In extremely rare circumstances anyone would denied access to their records, for example if providing access would create a significant risk to the person or to another person.

What if the records are not accurate?

We make every effort to ensure that all of the information is recorded accurately. If an inaccuracy is identified, a person can request that the information be corrected, and a note will be made to reflect this on the file.

Retaining information

We retain patient records for a minimum period of 16 years, or as otherwise required by law and professional regulations.

How do we dispose of information when it is no longer required?

When information is no longer required, it is destroyed in an irreversible and secure manner, in accordance with set procedures of the College of Physicians and Surgeons of BC that govern the storage and destruction of personal information.

Accuracy

PHS HealthCare staff will work to ensure that the information we collect is as accurate and complete as possible.

Individuals may request that PHS HealthCare correct any errors or omissions in their personal information that is under our control.

Safeguards

Safeguards are in place to protect the security of personal information. These safeguards include a combination of physical, technological and administrative security measures that are appropriate to the sensitivity of the information. These safeguards are aimed at protecting personal information against loss or theft, as well as unauthorized access, disclosure, copying, use or modification.

Administrative

Data is recorded in our electronic health record. It is backed up every 24 hours.
All information is stored in a Canadian cloud.

- Our EMR access is by two password login, with a unique User Name, Password, and Second Level passcode.
- The login details are provided in person to new users, with a unique username and generic Password, and they are provided with instructions to immediately change their password and create a password known only to them.
- Users are not allowed to have their unique login to be used by anyone else.
- Students and other temporary users have an Expiry Date added to their logins, so that they are unable to access the EMR after their scheduled shifts have concluded.
- PHS staff who resign their position with us have their EMR login de-activated immediately.
- A Medical Office Assistant reviews the list of active EMR users regularly and de-activates those that have had no activity for 3 months or more.
- Staff will only access charts for clinical care.
- Staff will Log-off of OSCAR when they are not at their work station
- When charting, staff will indicate the source of clinical information. When the source of information is from someone other than the patient (eg: family, chart) indicate this in the documentation.
- All requests for clinical information or records will be directed to the Privacy Officer to assess. No staff will release records without a discussion with the Privacy Officer.
- Any clinical discussions or conversations that involve personal information do not occur in a public area where others may overhear.

- All EMR log ins are role based, with limitations on what information can be accessed depending on the person's role in the organization.

Physical

Our clinic has locked doors and is alarmed. We contract with a security company to monitor our clinic alarm, and contact police if the alarm is set off.

Any paper records are stored in locked filing cabinets.

There is restricted access to our clinical spaces; only clinical staff have access to this space.

Our spaces are set up to prevent snooping. For example, all computers are facing away from public spaces. Any computers in high traffic areas have screen protectors applied to the monitors.

Printers are located in a secure area that has no public access.

We have secure paper shredding boxes, and contract with a secure shredding company.

Paper Medical Records

When using paper medical records:

- Staff will only remove medical records from the practice when it is absolutely necessary for performing job duties.
- All staff are required to obtain approval from their supervisor before removing medical records from the practice.
- Staff will take only the minimum amount of personal information required to perform the task required. If the records are large, they will use a courier to transport them to their destination. When records are being transported a distance more than a few minutes away, place records in confidential folders, transport them in a secure container (such as a locked briefcase), and keep them under control at all times, including meal and break times.
- Staff will keep records locked in a desk drawer or filing cabinet when working from home to reduce unauthorized viewing and access by family members or friends.
- If transporting medical records by car, staff will keep them locked in the trunk before the start of the trip.
- Staff will never leave medical records unattended, even if they are stored in the trunk as these are no less accessible to thieves than the front seats.
- Staff will never examine medical records in public places where they may be viewed or accessed by unauthorized individuals (e.g., on public transit) or leave medical records open for view in hotel rooms (e.g., keep them in the hotel safe).
- Immediately return medical records to their original storage location upon returning to the practices, and securely destroy any copies that are no longer required.

Technological

The PHS EMR is stored on our secure cloud, in a Canadian database that meets the data sovereignty requirements of PHS funders, which are Public Bodies.

Our EMR uses a double password to log in.

All workstations are encrypted, and any communication between devices is encrypted, such as SSL/TLS, etc.

SRFax, our secured faxing solution, is a PIPA/FIPPA compliant solution. (www.srfax.com)

As a matter of process, when selecting solutions for EMR / Medical information, the PHS tend to opt for FIPPA compliant options.

Portable Devices

When accessing medical records on portable electronic devices, staff will:

- Avoid storing personal information on portable electronic devices unless absolutely necessary. Even then, only use encrypted PHS electronic devices.
- Wireless transfer of personal information or storage on cloud-based programs will also be protected by industry-standard encryption.
- Protect portable electronic devices containing personal information with a strong password and use a secure method, such as two-factor authentication, to grant user access.
- Keep portable electronic devices secure to prevent loss or theft (e.g., in a locked briefcase, desk drawer, container or room) and keep them under one person's control at all times, including meal and break times.
- If transporting portable electronic devices by car, lock them in the car trunk before the start of a car trip.
- Never leave portable electronic devices unattended, even if stored in the trunk.
- Remove all sensitive personal information when no longer needed from portable electronic devices using a digital wipe utility program (do not rely on the delete function as the information may still remain on the device).

Electronic Records

When accessing medical records on home computers or portable electronic devices staff will:

- Avoid storing any personal information on the hard drive of a home computer.
- Never use public computers or wireless networks to connect to the practice network as these are not secure.
- Never use a laptop or home computer that is shared with other individuals, including family members and friends.
- Never send documents containing personal information to or from a personal or otherwise unsecured email address.
- Always log off from a laptop or home computer when not in use.
- Set an automatic log out to occur after a period of inactivity.
- Lock home computers that are used for work-related purposes to a table or other stationary object with a security cable.
- Keep home computers in a room with restricted access.
- Use strong, up-to-date, industry-standard encryption and password protection for any personal information that must be stored on hard drives.

- Ensure that laptops and home computers have, at a minimum, a personal firewall, anti-virus protection, and anti-spyware protection.
- Ensure the latest updates and security patches are regularly installed.
- Never store information on personal devices such as a cell phone or personal computer.
- If electronic information needs to be stored outside OSCAR EMR, it can only be on a secure, encrypted, password protected PHS computer, and the document must be also password protected.

Systems

Theft:

If a person were to steal the physical computers, they would not be able to access any medical information.

If a device were to be stolen, it would be remotely wiped of all data.

We work closely with our EMR support service provider, NERDS BC to maintain up to date versions of our EMR to optimise security.

Communication

PHS HealthCare is sensitive to the privacy of personal information and this is reflected in how we communicate with our patients, others involved in their care and all third parties.

We protect personal information regardless of the format.

We use specific procedures to communicate personal information by

Telephone
We respect patient preference with regards to phone messages is taken into consideration.
Unless authorized, we only leave our name and phone number on message for patients on voicemail or verbal messages for phone numbers where the person has given us permission to use.

Fax
We use SRFax, our secured faxing solution, which is a PIPA/FIPPA compliant solution. (www.srfax.com)

Our fax machine is located in a supervised area.

We use pre-programmed numbers with clear identification by name or title, to ensure fax received by proper recipient.

Post/Courier

When we send information by mail or by courier, is it in a sealed envelope and marked as confidential.

Access to Personal Information

Individuals can access their own personal information. They can also access information about how their personal information is being used.

A request for access to information must be made in writing.

Individuals must prove their identity before the information will be released to them.

We will charge a minimal fee for releasing information to account for the work involved.

We will provide this information within 30 days.

Challenging Compliance

Individuals can ask about our PIPA compliance, and have a right to complain.

Complaints can be made in writing or by phone. Written complaints should be sent to the PHS HealthCare Clinic:

350 Columbia Street
Vancouver, BC
V6A 4J1

Or by calling the PHS HealthCare Clinic at 604-879-7906

Complaints should be to the attention of the PHS HealthCare Privacy Officer: Dr. Christy Sutherland

If an individual is not satisfied with how PHS HealthCare performs its duties under PIPA, or wishes to seek a review of our response to their access or correction request, they can contact The Office of the Information and Privacy Commissioner of British Columbia at www.OPIC.BC.ca, or by Telephone (250) 387-5629.

Protocol for Privacy Breach

A privacy breach includes the loss of, unauthorized access to, or unauthorized collection, use, disclosure, or disposal of personal information.

Step 1:

Reporting

Any privacy breach should be reported immediately to Dr. Christy Sutherland, the privacy officer. If Dr. Sutherland is not available, her delegate will fill this role.

Step 2:

Contain

The Privacy Officer, Supervisor, and (designated) staff will take immediate steps to contain the breach, including seeking assistance from Information Technology (the systems team).

For example:

·Stop unauthorized practice;
·Recover records;
·Shut down the system that was breached;
·Revoke or change computer access codes;
·Correct physical security weaknesses

The Privacy Officer will keep the Executive apprised of any breaches and their management. The Privacy Officer will liaise with the Information and Privacy Commissioner and the Director of Communications with respect to any public comments regarding a breach.

The Privacy Officer will document the breach and perform a risk evaluation.

Step 3:

Notification

Individuals will be notified as soon as possible about the breach.

Notification of affected individuals will include:
·Date of the breach;
·Description of the breach;
·Description of the personal information involved;
·Risk(s) to the individual;
·Steps taken to control or reduce the harm;
·Future steps planned to prevent further privacy breaches;
·Steps the individual can take to control or reduce the harm;
·Contact information of the OIPC's Privacy Office

Step 4

Security Safeguards and Prevention Strategies

The Privacy Officer, Supervisor, or designated staff will determine whether any improvements or changes to security safeguards are needed as a result of the breach, including determining whether additional preventative measures are necessary.

Privacy Management Program

Internal Reporting structure

Any privacy concerns should be reported directly to Dr. Christy Sutherland, the Privacy Officer for PHS HealthCare. If she is not available, report to her delegate.

Privacy and Security Training

All nursing staff adheres to the Privacy and Confidentiality standards of practice per the BCCNP:
https://www.bccnp.ca/Standards/RN_NP/PracticeStandards/Pages/privacy.aspx

All clinical staff complete: Privacy and Confidentiality (all PHSA agencies) e-learning module through the Provincial Health Services Authority Learning Hub. All staff sign the Undertaking of Confidentiality and Security Form for PharmaNet use with PHS.

Staff confidentiality agreement

All staff are contractually required to adhere to our privacy policy.

Employees will also sign the confidentiality agreement.

Physician contracts include requirement to abide by PHS privacy policy.

Ongoing Education and Program Development

The PHS Privacy Officer will provide ongoing advocating for privacy in our organization. This includes ongoing education and support for staff to maintain a high standard of privacy.

Our privacy policy and program will be reviewed annually.