RISE Community Health Centre Privacy Policy

Privacy Officer: Sonja Rietkerk, Nurse Practitioner & Clinical Lead
Phone: 604-558-8090 Ext 1
Address: 5198 Joyce St, Vancouver, BC, V5R 4H1

Introduction

RISE Community Health Centre operates within Collingwood Neighborhood House Society (CNH). 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 RISE Community Health Centre (CHC) collects about the clients for whom we provide care.

As a team, we foster a culture of privacy, and work in compliance with PIPPA. RISE CHC and CNH are 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 RISE CHC Privacy Policy. It is to inform staff and clients 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 RISE CHC staff shared drive, on our website, and clients or the public will be provided a paper copy upon request.

Background

<u>Types of information we are collecting:</u>

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

- 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 primary care.

Who are we collecting personal information from?

People who present to RISE CHC at our main location and/or during outreach requesting to become a client of RISE CHC and are requesting primary care services.

What is the purpose of collecting the information and how will it be used?

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

Sensitivity of collected information

High sensitivity.

Where is personal information documented?

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.

Who has custody of the information?

Collingwood Neighborhood House Society has custody of the medical records.

Consent to collect information

By virtue of seeking care from RISE CHC, consent is implied (assumed) for personal information to be used by RISE CHC 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 primary care.

In circumstances such as research, where information is requested from an external party, we will obtain additional consent from each individual before sharing information. All clients have the right to refuse to participate in research and this will not affect their care with RISE CHC.

Disclosing information

Disclosure to other health care providers:

A client's implied consent extends to RISE CHC sharing personal information with other providers involved in a client's care, including (but not limited to) other nurse practitioners, physicians and

specialists, pharmacists, lab technicians, dietitians, physiotherapists, nurses, social workers, counsellors, community health workers and occupational therapists.

Disclosures authorized by law:

RISE CHC will only disclose personal information where authorized by PIPA or required by law (for example, in the event of a court order, subpoena, search warrant, or if we think a child or youth under 19 years of age is being abused or neglected).

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

Express consent from each client 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.

Client Rights to Access Records

- Clients have the right to access their record in a timely manner. Client may request a copy of their record, by signing the Release of information/medical record form (ROI).
- Client requests for medical record can be made in writing to a RISE CHC staff (see office address at the top of our Privacy Policy). Records must be picked up in person, and will not be sent via email.
- Clients must prove their identity before the information will be released to them
- We will provide this information within 30 days.
- In extremely rare circumstances anyone could be denied access to their records, for example if providing access would create a significant risk to the person or to another person.

Retaining information

We retain client records in our OSCAR data base for a minimum period of 16 years, or as otherwise required by law and professional regulations.

When information is no longer required, it is destroyed in an irreversible and secure manner, in accordance with each health care professional appropriate college and the Health Professions Act (and Social Workers Act) that govern the storage and destruction of personal information.

Accuracy

RISE CHC staff will work to ensure that the information we collect is as accurate and complete as possible. Individuals may request that RISE CHC correct any errors or omissions in their personal information that is under our control and a note will be made to reflect this on the file.

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.
- RISE CHC staff who resign their position with us have their EMR login de-activated immediately.
- RISE CHC Manager 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 the provision of primary 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 client (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.

Physical

- RISE Community Health Centre has locked doors and is alarmed. We contract with a security company to monitor our 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 staff work spaces; only Community Health Centre staff have access to this space.

- Our spaces are set up to prevent snooping. For example, all computers are facing away from public spaces.
- 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

The vast majority of RISE CHC records are electronic. 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 secured and stored in a safe space 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 lock before the start of the trip.
- Staff will never leave medical records unattended, even if they are securely stored.
- Staff will never examine medical records in public places where they may be viewed or accessed by unauthorized individuals (e.g., on public transit).
- 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 RISE CHC EMR is stored on our secure cloud, in a Canadian database that meets the data sovereignty requirements of RISE CHC 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 RISE CHC chooses 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, they will only use encrypted RISE CHC 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 and keep them under on person's control at all times, including meal and break times.
- If transporting portable electronic devices by car, lock them in the car 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).

Remote Work

When accessing medical records on home computers or portable electronic devices RISE CHC staff will follow the CNH and RISE CHC Remote Work policies which include:

- Employees must have the CNH remote desktop installed on the computer to work remotely.
- Staff must work while logged onto the remote desktop, which is firewall protected.
- Employees must have a dedicated and secure workspace at their remote location which is set up to maintain client's confidentiality (ex: not working in a public space or in a room where housemates or family can hear conversations or see your computer screen).
- Remote employees must have access to secure (password protected).
- All client related documents, records, and materials must be securely stored in Electronic Medical record system or on the RISE CHC drive as appropriate.
- Ensure that laptops and home computers have, at a minimum, a personal firewall, antivirus 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 RISE CHC computer, and the document must be also password protected.

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, OSCAR Open OSP to maintain up to date versions of our EMR to optimise security.

Communication

RISE CHC is sensitive to the privacy of personal information and this is reflected in how we communicate with our clients, 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, fax, post and email as follows:

Telephone

We respect client preference with regards to phone messages is taken into consideration. Unless authorized, we only leave our name and phone number on message for clients 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). We use E-Faxes, so faxes go directly to and from our OSCAR EMR.

Post/Courier

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

Email

The RISE CHC generic email has an auto reply as follow:

"Thank you for your email. This email is not checked regular and is used for administrative purposes only. To protect your privacy, and the privacy of our clients please note, this is not a way to contact the medical team. Please do not send medical information to this email.

*If you are a current **RISE CHC primary care client** and want to communicate about appointment bookings, prescription refills, or to speak with a staff member about a concern, please book an appointment online at https://risecentre.cortico.ca/ or call Community Health Centre reception at 604-558-8090 EXT 1 during regular business hours. If you are another **medical or social service provider** please fax client related information to 236-317-4270 or email to risereception@cnh.bc.ca."*

This is in order to prevent clients or external partners from emailing confidential information to non-medical branches of the organization.

If a non-medical RISE CHC staff is sent medical information by email, they will reply with a standardized message:

"Thank you for your email. This email address is for RISE CHC overall, not for the Primary Care Clinic. If you have a medical concern, please call the clinic at 604-604-558-8090 Ext: 1 or email risereception@cnh.bc.ca"

Clients and other health care service providers can send information to RISE CHC by emailing risereception@cnh.bc.ca, and they will reply with the standardized message:

"Thank you for your email. This email is not checked frequently. If you are emailing to request to speak to a staff, for a prescription refill or to book/change an appointment, please call the RISE Community Health Centre reception at 604-558-8090 Ext: 1 or book your appointment online at https://risecentre.cortico.ca/

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 RISE CHC Or by calling the RISE CHC Clinic. The formal complaint form can be found at: https://www.cnh.bc.ca/wp-content/uploads/2024/06/Non-Staff-Complaint-Procedure-Form.pdf

Complaints should be to the attention of the RISE CHC Privacy Office.

If an individual is not satisfied with how RISE CHC 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 the privacy officer. If privacy officer is not available, her delegate (CHC Manager) 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 breach
- Revoke or change computer access codes;
- Correct physical security weaknesses

The Privacy Officer will keep the RISE CHC Manager, Director, Mercury and OSCAR Tech support apprised of any breaches and will liaise with the Information and Privacy Commissioner s with respect to any public comments regarding a breach. The Privacy Officer will document the breach and perform a risk evaluation.

Step 3: Notification

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

- Notification of affected client will include
- Date of the breach
- Description of the breach
- Description of the personal information involved
- Risk(s) to the client
- Steps taken to control or reduce the harm
- Future steps planned to prevent further privacy breaches
- Steps the client can take to control or reduce the harm
- Contact information of the Office of information and privacy commissioner Privacy Office

Step 4: Security Safeguards and Prevention Strategies

The Privacy Officer, RISE CHC Management team, 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 the Privacy Officer for RISE CHC. If not available, report to delegate (RISE CHC Manager).

Privacy and Security Training

All RISE staff are responsible for meeting the legislated requirements for the collection, storage, use, and disclosure of personal and health information. Each health professional is regulated by their appropriate college and under the Health Professions Act (and Social Workers Act).

All clinical staff complete: Privacy and Confidentiality e-learning module through the Provincial Health Services Authority Learning Hub.

Staff confidentiality agreement

- All staff are contractually required to adhere to our privacy policy and confidentiality agreement.
- All staff sign the Undertaking of Confidentiality and Security Forms including: Careconnect, Medinet and others BC Services applications used within RISE CHC.

Ongoing Education and Program Development

The RISE CHC 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.

Reviewed: February 21st, 2024
RISE Privacy Officer: Sonja Rietkerk- Clinical Lead & Nurse Practitioner
RISE CHC Manager, Nilam Khoja
RISE CHC Director, Sandra Bodenhamer