Virtual Health Care & Privacy Policy

Last Updated: February 2023

Introduction

Ontario's Personal Health Information Protection Act (PHIPA) imposes obligations with respect to the collection, use, and disclosure of personal health information. This Privacy Policy governs the manner in which Jennifer Lane & Kayleen Edwards, operating as Roots in Wellness collects, uses, maintains and discloses information Outlined within our Virtual Health Care Policy are important details related to your personal information.

Definitions

Definitions as per Personal Health Information Protection Act (PHIPA)
https://www.ipc.on.ca/wp-content/uploads/2015/11/phipa-faq.pdf

Health Information Custodian: "PHIPA defines a custodian is a person or organization listed in PHIPA that, as a result of his, her or its power or duties or work set out in PHIPA, has custody or control of personal health information" At Roots in Wellness, Jennifer Lane and Kayleen Edwards operate as the Health Information Custodian, depending on who the client is seeing. Kayleen Edwards is the Health Information Custodian for herself, students working under her supervision, and associates working under her supervision. Jennifer Lane is the Health Information Custodian for herself, students working under her supervision, and associates working under her supervision. Should you require clarification on who is the Health Information Custodian, please email info@rootsinwellness.ca.

Agent: “PHIPA defines an agent to include any person who is authorized by a custodian to perform services or activities in respect of personal health information on the custodian’s behalf and for the purposes of that custodian. At Roots in Wellness, our sub-contracted therapists, administrative team and students operate as agents.

Personal Health Information (PHI):” Personal health information is “identifying information” about an individual, whether oral or recorded if the information:

- relates to the individual’s physical or mental condition, including family medical history,
- relates to the provision of health care to the individual,
- is a plan of service for the individual,
- relates to payments, or eligibility for health care or for coverage for health care,
- is the individual’s health number or
- identifies a health care provider or a substitute decision-maker for the individual.”

Electronic Records: Electronically stored documents that include client personal health information. Electronic Records are kept securely on the Jane software platform.

Adherence to PHIPA

At Roots in Wellness, we are dedicated to operating in adherence with PHIPA . This includes, but is not limited to:

a) Ensuring that our clients personal health information is collected, used, disclosed and disposed of properly, to the best of our abilities;
b) Ensuring that our clients personal health information and electronic records remain confidential;
c) Ensuring that Agents at Roots in Wellness are aware of their responsibilities in adhering to PHIPA

In addition to adherence to PHIPA, as independent contractors, each Agent is responsible for ensuring their adherence to their respective colleges.

Access to Information by HIC & Agents

Full Access

At Roots in Wellness the individual with full access to PHI is either Jennifer Lane, Registered Psychotherapist #004847, or Kayleen Edwards, Registered Psychotherapist #004288. We are the dedicated Health information Custodians (HIC) and abide by strict confidentiality guidelines in adherence to PHIPA. While Jennifer and Kayleen have full access to PHI, we will not access client clinical notes unless absolutely necessary to do so to execute their duties as the HIC.
In the event that PHI is accessed by the HIC, a chart entry will be added to the client file which outlines the detail of the access including the following:

a) HIC Name
b) Date & time of PHI access
c) What was viewed, handled or modified on the client file.

The HIC is responsible for regularly auditing Logs of accidental access which can be requested by the information and Privacy Commissioner of Ontario.

Practitioner-Only Access

At Roots in Wellness the individuals with practitioner-only access include subcontracted therapists and students.

Practitioner-only access on Jane Practice Management Software permits the Agent to only view or modify the client charts of their own clients. Practitioner-only access does not permit clinician to view the client charts of other clinicians at Roots in Wellness.

In the event that another clinicians chart notes are accidentally accessed, a chart entry will be added to the client file which outlines the detail of the access including the following:

a) Accessing Clinician Name, & HIC name
b) Date & time of PHI access
c) What was viewed, handled or modified on the client file

Administrative Level Access

At Roots in Wellness the individuals with administrative-only access include Administrative & Non-Clinical Contractors.

Administrative level access on Jane Practice Management Software means that the individual will be prohibited from accessing any client clinical notes for any reason unless directed and given access by the HIC. Under this access level, any roles that require access to Jane Practice Management Software, including accessing client profiles, billing and/or appointment information will be kept to a minimum.

In the event that another clinicians chart notes are accidentally accessed, a chart entry will be added to the client file which outlines the detail of the access including the following:

a) Accessing Clinician Name, & HIC name
b) Date & time of PHI access
c) What was viewed, handled or modified on the client file

Safeguards

Listed below are various safeguards that we have implemented to protect your PHI. We regularly review these safeguards to ensure that we are doing all that we can to protect your PHI.

https://www.ipc.on.ca/wp-content/uploads/2021/02/virtual-health-care-visits.pdf

Technical safeguards:

- use only organization-approved email, messaging, or videoconferencing accounts, software, and related equipment. The HIC and Agents are required to use only the @rootsinwellness.ca email domain, JANE (EMR) software system, and Signal chat software.

- use firewalls and protections against software threats are recommended for use by all agents. Both the HIC and Agents are urged to implement adequate firewall and antivirus protection on their electronic devices.

- regularly update applications with the latest security and anti-virus software. JANE (EMR) regularly updates and both the HIC and Agents are urged to regularly update their electronic devices.

- encrypt data on all mobile and portable storage devices, both in transit and at rest. Both the HIC and Agents use encrypted devices.

- maintain, monitor, and review audit logs. The HIC conducts regular audits, keeps an up-to-date audit log.

- use and maintain strong passwords. All electronically stored PHI is password protected.

- review and set default settings to the most privacy protective setting. Jane Settings are set for enhanced privacy and Agents are encouraged to adjust privacy settings on their electronic devices.

- If your Jane calendar is synced externally from the platform to your phone's calendar, or another app's calendar feature, you must ensure it is password protected or that it hides client information.

Administrative safeguards:

- ensure team and other agents are properly trained to use secure email, messaging, and video conferencing platforms.

- ensure team and other agents are well aware of their ongoing obligation to avoid collecting, using or disclosing more personal health information than is necessary

- ensure confidentiality agreements contain explicit provisions dealing with team member's' and other agents' obligations when using secure email, messaging, or videoconferencing to deliver virtual health care

- all email communication between the HIC or agents and clients should be done through the Roots in Wellness Domain and includes a confidentiality statement outlining the privileged nature of the information, intended only for the recipient, the process for

destroying information should it be the incorrect recipient and lastly, that sensitive information should not be shared via email.

- Limiting Data in written communication. To minimize use of PHI, the HIC and agents use, wherever possible, client initials or their Jane Client I.D instead of identifying information such names, phone numbers etc.

- recommending that clients use a password-protected email address that only they can access.

Physical safeguards:

- keep all technology containing personal health information, such as desktop computers and servers, in a secure location

- keep portable devices containing personal health information, such as smartphones, tablets, and laptops, in a secure location, such as a locked drawer or cabinet, when they are unattended

- restrict office access, use alarm systems, and lock rooms where equipment used to send, receive or store personal health information is kept

- do not lend technology containing personal health information to anyone without authorization

- ensure there are no unauthorized persons in attendance or within hearing or viewing distance

- any physical copy of phi that is not electronically stored needs to be physically locked away when not in use, or destroyed within 24 hours of creation.

Additional safeguards for video conferencing

- As a best practice, both the custodian and the client should join the videoconference from a private location using a secure internet connection. This includes using a closed, soundproof room or an otherwise quiet and private place and having window coverings where and as appropriate. Use headphones rather than the speaker on the device to prevent being overheard by others, and be mindful of where screens are positioned.

- Once logged into the videoconference, the custodian should check the meeting settings to ensure the meeting is secure from unauthorized participants. At the start of an initial visit, the custodian should verify the identity of the client. The custodian should also inquire if anyone is accompanying the client and confirm the consent of the client. When videoconferencing, custodians must use sufficiently high-quality sound and resolution to ensure they are able to collect information (including verbal and non-verbal cues) that is as accurate and complete as is necessary for the purpose of providing health care

Withdrawal of Consent

https://www.ipc.on.ca/wp-content/uploads/resources/fact-08-e.pdf

Clients reserve the right to withdraw their consent at any point. Should a client wish to withdraw their consent, therapy services will be terminated. As per the Information and Privacy Commissioner of Ontario, we will make an entry into the chart logging the withdrawal. We will then discuss with the client details around 'lock boxing' their information, what this means for their care and their rights for the future.

Privacy Breach Protocol

In the event that there is a security breach, Roots in Wellness has a comprehensive privacy breach protocol that involves 4 steps, generally outlined below. It is our commitment to ensure that your PHI remains confidential and is collected, used, disclosed and disposed of properly to the best of our abilities, however; in the unlikely event that a privacy breach does occur, we will adhere to our privacy breach protocol to ensure a timely remediation of said breach.

There is an obligation under PHIPA to notify affected individuals of a privacy breach (e.g. the theft, loss or unauthorized use or disclosure of personal health information) (ss. 12(2)). Custodians are also required to notify such individuals of their right to make a complaint to the Information and Privacy Commissioner.

If a privacy breach is suspected or known to have occurred, take the following action:

Step 1: Ensure the Contact Person is informed of the breach.

- Consider whether the Commissioner must or should be notified.
- A report must be formally made as a record of all privacy breaches will be maintained.

Step 2: Contain the Breach

- Retrieve hard copies of personal health information that have been disclosed
- Ensure no copies have been made
- Take steps to prevent unauthorized access to electronic information (e.g., restrict access, change passwords, temporarily shut down system)

Step 3: Notify affected individuals (consult with HIC to decide who will inform)

- Consider the most appropriate way to notify affected individuals in light of the sensitivity of the information (e.g., by phone, in writing, at the next appointment)
- Provide the organization's contact information (HIC) in case the individual has further questions

Step 4: HIC will further Investigate and remediate the problem

- Conduct an internal investigation
- Determine what steps should be taken to prevent future breaches (e.g. changes to policies, additional safeguards required)
- Report the results of the investigation to the relevant regulatory College if appropriate or required
- Ensure staff is appropriately trained and conduct further training if required.

ROOTS IN WELLNESS

Record Retention Policy

In accordance with PHIPA, we ensure that any and all records are retained only for the period in which they are required to be retained (in accordance with regulatory colleges CRPO or OCSWSSW). Following this retention period, we ensure any PHI is securely destroyed.

We need to retain personal information for some time to ensure that we can answer any questions clients might have about the services provided and for our own accountability to external regulatory bodies. However, in order to protect client privacy, we do not want to keep personal information for too long. We keep our client files for at least ten years from the date of the last client interaction or from the date the client turns 18.

We destroy paper files containing personal health information by cross-cut shredding. We destroy electronic information by deleting it in a manner that it cannot be restored. When hardware is discarded, we ensure that the hardware is physically destroyed or the data is erased or overwritten in a manner that the information cannot be recovered.

Complaints

The identification of a Contact Person is required to allow for consistent and professional regulations regarding any internal complaints. This organization's Contact Person is: Jennifer Lane, Clinical Director and Owner. Upon receiving a complaint:

- acknowledgement of receiving the complaint
- gather pertinent information
- interview parties involved
- determine what action, if any, will be taken
- communicate any decision to the complainant along with a summary of action
- advise complainant of their right to pursue additional action through the Information and Privacy Commissioner of Ontario

Questions or Concerns?

If you have questions or want to make a complaint about our privacy practices, please contact:

Jennifer Lane and Kayleen Edwards

info@rootsinwellness.ca