Privacy Policy - YSSN Agency (OP PR 0.1)

Version: 4

Document Owner: Scott Belisle	Policy Number	**OP PR 0.1**
	Original Date Created	**02/16/2016**
Category: Operations	Compliance	Click here to enter text.
Approver(s): Jean West (Manager), Kimberly Thorn (Manager)	Date Approved	**01/26/2018**

A. PRIVACY POLICY - YSSN

York Support Services Network (YSSN) is committed to client privacy and to protecting the confidentiality of the health information we hold.

YSSN is designated as a **Health Information Custodian** under the *Personal Health Information Protection Act, 2004* ("**PHIPA**").

The Health Information Custodian is accountable for compliance with PHIPA and the protection of health records.

This Privacy Policy acts as the articulation of the privacy practices and standards to guide the Health Information Custodian, staff members and any other agents (students, subcontractors). There are additional privacy policies that are included by reference to this Privacy Policy and are listed at **Appendix A**. All staff members agree to abide by those policies as well.

PRINCIPLE 1: Accountability for Personal Health Information

The Health Information Custodian is responsible for any personal health information held. The Privacy Officers are accountable for compliance with this Privacy Policy and compliance with PHIPA. The following individuals have been designated as the Privacy Officers:

- **Marilyn Graham (905)-898-6455 ext.2240**
- **Scott Belisle (905)898-6455 ext.2371**

Our commitment to privacy is demonstrated by adherence to privacy policies and procedures to protect the personal health information we hold, and through our education to our staff and any others who collect, use or disclose personal health information on our behalf about their privacy responsibilities.

PRINCIPLE 2: Identifying Purposes for Collecting Personal Health Information

We collect personal health information for purposes related to direct client care, administration and management of our programs and services, statistical reporting, research, meeting legal obligations and as otherwise permitted or required by law.

When personal health information that has been collected is to be used for a purpose not previously identified, the new purpose will be identified prior to use. Unless the new purpose is permitted or required by law, consent will be required before the

information can be used for that purpose.

PRINCIPLE 3: Consent for the Collection, Use and Disclosure of Personal Health Information

We require consent in order to collect, use, or disclose personal health information. However, there are some cases where we may collect, use or disclose person health information without consent as permitted or required by law.

Express Consent

Where possible, YSSN requires written consent but accepts other ways clients may give consent including:

- Verbal – in person or over the telephone (YSSN staff are to document receiving the consent)
- A letter from a client to YSSN
- Electronic means where YSSN is able to sufficiently identify the person

See YSSN's "*Access and Correction Policy - Release of Consumer Information*".

Should a client wish his/her lawyer, insurance company, family, employer, landlord or other third party individuals or agencies (non-health care providers) to have access to his/her health record, the client must provide verbal or written consent to this effect, which will be communicated in accordance with YSSN's policy: "*Access and Correction Policy – Release of Client Information*".

Service Indicators:

- Staff reviews the rights of clients serviced and responsibilities of the agency during the orientation to service [see: YSSN Policies – Orientation to Service – Welcome to YSSN Package] [see YSSN PHI Privacy Statement]
- Staff reviews the purpose for collecting, using and disclosing personal health information with the client
- Staff adheres to requirements of the Consent Management Process [see: Service Delivery Manual(s)]

Implied consent (disclosures to other health care providers for health care purposes) - Circle of Care

Client information may also be released to a client's other health care providers for health care purposes (within the "circle of care") without the express written or verbal consent of the consumer as long as it is reasonable in the circumstances to believe that the client wants the information shared with the other health care providers. No client information will be released to other health care providers if a client has stated he/she does not want the information shared (for instance, by way of the placement of a "restriction" on his/her health records).

A client's request for treatment constitutes implied consent to use and disclose his/her personal health information for health care purposes, unless the consumer expressly instructs otherwise.

Who can be in the "circle of care" includes (among others providing direct client care if

authorized by PHIPA):

Outside of the Organization:

- Hospitals
- Community Care Access Centres
- Community Health Centres
- Long-term care homes
- Family health teams
- Ambulance
- Pharmacists
- Laboratories
- Regulated health professionals in sole practice or group
- Social workers and social service workers in sole practice or group
- A centre, program or service for community health or mental health whose primary purpose is the provision of health care

No Consent

There are certain activities for which consent is not required to use or disclose personal health information. These activities are permitted or required by law. For example, we do not need consent from clients to (this is not an exhaustive list):

- Plan, administer and manage our internal operations, programs and services
- Engage in quality improvement, error management, and risk management activities
- Participate in the analysis, administration and management of the health care system
- Engage in research (subject to certain rules)
- Teach, train and educate our staff and others
- Compile statistics for internal or mandatory external reporting
- Respond to legal proceedings
- Comply with mandatory reporting obligations

A list of mandatory reporting obligations is found in YSSN's "*Access and Correction – Release of Client Information Policy*".

If a staff member has questions about using and disclosing personal health information without consent, they can ask one of the Privacy Officers.

Withholding or Withdrawal of Consent

If consent is sought, a client may choose not to give consent ("withholding consent"). If consent is given, a client may withdraw consent at any time, but the withdrawal cannot be retrospective. The withdrawal may also be subject to legal or contractual restrictions and reasonable notice.

Lockbox

PHIPA gives clients the opportunity to restrict access to any personal health information or their entire health record by their health care providers within the Agency, or by external health care providers. Although the term "lockbox" is not found in PHIPA, lockbox is commonly used to refer to a client's ability to withdraw or withhold consent for the use or disclosure of their personal health information for health care purposes. See the YSSN "*Lockbox Policy*" for details of how the

lockbox works.

PRINCIPLE 4: Limiting Collection of Personal Health Information

We limit the amount and type of personal health information we collect to that which is necessary to fulfill the purposes identified.

Personal health information may only be collected within the limits of each staff member's role. Staff members should not initiate their own projects to collect new personal health information from any source without being authorized by the Agency or one of the Privacy Officers.

PRINCIPLE 5: Limiting Use, Disclosure and Retention of Personal Health Information Use

Personal health information is not used for purposes other than those for which it was collected, except with the consent of the client or as permitted or required by law.

Personal health information may only be used within the limits of each staff member's role. Staff members may not read, look at, receive or otherwise use personal health information unless they have a legitimate "need to know" as part of their position. If a staff member is in doubt as to whether an activity to use personal health information is part of his/her position, he/she should ask one of the Privacy Officers. For example, self-directed learning (randomly or intentionally looking at health records for self-initiated educational purposes) is not allowed without specific authorization.

Disclosure

Personal health information is not disclosed for purposes other than those for which it was collected, except with the consent of the consumer or as permitted or required by law.

Personal health information may only be disclosed within the limits of each staff member's role. Staff members may not share, talk about, send to or otherwise disclose personal health information to anyone else unless that activity is an authorized part of their position. If a staff member is in doubt whether an activity to disclose personal health information is part of his/her position, he/she should ask one of the Privacy Officers.

Retention

Health records are retained as required by law and professional regulations and to fulfill our own purposes for collecting personal health information. YSSN is required to keep clinical records for a minimum of **10 years** after the record is closed and for 10 years after a child's eighteenth birthday. The destruction date is revised if service is reactivated.

***Note*: Should a legal investigation take place, YSSN's Privacy Officers are to be notified and the destruction of all records will cease until the investigation is completed.**

Personal health information that is no longer required to fulfill the identified purposes is destroyed, erased, or made anonymous safely and securely. Please see YSSN's "Safeguards for Client Information *Guidelines*".

PRINCIPLE 6: Accuracy of Personal Health Information

We will take reasonable steps to ensure that information we hold is as accurate, complete, and up to date as is necessary to minimize the possibility that inappropriate information may be used to make a decision about a client.

PRINCIPLE 7: Safeguards for Personal Health Information

We have put in place safeguards for the personal health information we hold, which include:

- Physical safeguards (such as locked filing cabinets and having a locked file room);
- Organizational safeguards (such as permitting access to personal health information by staff on a "need-to-know" basis only); and
- Technological safeguards (such as the use of passwords, encryption, and audits).

We take steps to ensure that the personal health information we hold is protected against theft, loss and unauthorized use or disclosure. The details of these safeguards are set out in the YSSN's "Safeguards for Client Information Guidelines".

We require anyone who collects, uses, or discloses personal health information on our behalf to be aware of the importance of maintaining the confidentiality of personal health information. This is done through: the signing of confidentiality agreements, privacy training, and contractual means.

Care is used in the disposal or destruction of personal health information, to prevent unauthorized parties from gaining access to the information.

PRINCIPLE 8: Openness about Personal Health Information

Information about our policies and practices relating to the management of personal health information is available to the public, including:

- Contact information for our Privacy Officers, to whom complaints or inquiries can be made;
- The process for obtaining access to personal health information we hold, and making requests for its correction;
- A description of the type of personal health information we hold, including a general account of our uses and disclosures; and
- A description of how a client may make a complaint to YSSN or to the Information and Privacy Commissioner of Ontario.

PRINCIPLE 9: Client Access to Personal Health Information

Clients may make written requests to have access to their records of personal health information, in accordance with the Agency's **"***Access and Correction Policy – Release of Client Information*".

We will respond to a client's request for access within reasonable timelines and costs to the client, as governed by law. We will take reasonable steps to ensure that the requested information is made available in a format that is understandable.

Clients who successfully demonstrate the inaccuracy or incompleteness of their personal health information may request that we amend their information. In some cases instead of making a correction, clients may ask to append a statement of disagreement to their file.

***NOTE*: In certain situations, we may not be able to provide access to all the personal health information we hold about a client. Exceptions to the right of access requirement will be in accordance with law. Examples may include information that could reasonably be expected to result in a risk of serious harm or the information is subject to legal privilege.**

PRINCIPLE 10: Challenging Compliance with the Organization's Privacy Policies and Practices

Any person may ask questions or challenge our compliance with this policy or with PHIPA by contacting our Privacy Officers.

We will receive and respond to complaints or inquiries about our policies and practices relating to the handling of personal health information. We will inform clients who make inquiries or lodge complaints of other available complaint procedures.

We will investigate all complaints. If a complaint is found to be justified, we will take appropriate measures to respond.

The Information and Privacy Commissioner of Ontario oversees our compliance with privacy rules and PHIPA. Any individual can make an inquiry or complaint directly to the Information and Privacy Commissioner of Ontario by writing to or calling:

2 Bloor Street East, Suite 1400
Toronto, Ontario M4W 1A8 Canada
Phone: 1 (800) 387-0073 (or 416-326-3333 in Toronto)
Fax: 416-325-9195
www.ipc.on.ca

B. Related Documents

This section specifies any documents, forms and templates associated with the **Privacy Policy**. Click on the following links to access documents.

- Access and Correction Policy (Privacy) PR 02
- Lock Box Procedure - Privacy Policy
- PHIPA - Privacy Breach Protocol/Policy (OP PR 1.2)
- Safeguards for Client Information Guidelines - Privacy Policy - Agency (PR 1.0)