	Operating Manual		
	Section: **Privacy**	Policy Name: **Privacy Policy - Yorktown Family Services**	Policy #: ORG **8.1**
	Implementation Date: **August 2007**	Revision Dates: **August 2007** **August 2011** **February 2015** **November, 2019**	Last Review Date: **August 2008** **August 2011** **February 2015** **October 2019** **July 2023**

POLICY:

Yorktown Family Services recognizes the sensitivity of an individual's personal health information and therefore, is committed to respecting, safeguarding and protecting clients' personal health information in compliance with the *Personal Health Information Act, 2004.* This Act requires that all personal health information is kept private and secure. Yorktown Family Services collects, uses, and shares personal health information and must therefore comply with the Act. This policy applies to all Agency employees. All personal and confidential information, regardless of format or how it is obtained, stored or recorded, is protected by this policy and applies while in the course of working and conducting business for or on behalf of the Agency, including when off-duty, and extends beyond the completion of the employment or business relationship.

DEFINITIONS:

Within this policy, the law is referred to as "PHIPA", Personal Health Information Protection Act. Personal Health Information is referred to as "PHI" or "information". This is identifying information that relates to a client's physical or mental health, including his or her health history as well as his or her family's health history.

Within the Act, health professionals, institutions and agencies that hold personal health information are referred to as "Health Information Custodians", abbreviated to "HIC's" or "custodians". Yorktown Family Services is a HIC and is responsible for the PHI that is collected, used, maintained and shared, as set out in this policy.

"Express Consent" means permission that must be specifically obtained from the client. "Implied Consent" means that staff of the agency may conclude from the surrounding circumstances that the client would agree to the collection, use or disclosure of his or her PHI.

What Information is Collected from the Client?

Clients may be asked to provide whatever information about themselves or their families that is needed in order to provide the necessary care or treatment. This may include the families' health history as well as information about the care or treatment the client has received.
The information that is collected will be for the purpose of the main activities of the agency:

- Treatment planning;
- Collaborating and working as part of a multi-disciplinary team to provide care to clients;
- Providing a comprehensive and flexible range of services from prevention and early intervention to treatment programs for children, youth and their families;
- Teaching and fostering a learning environment; and,
- Empowering and enabling individuals to foster healthy relationships.

The PHI may also be used for quality assurance, evaluation, accreditation and licensing processes. Information will only be collected indirectly, that is, from other family members or professionals, if necessary to provide the health care and treatment, with the client's consent or if permitted to do so by law.

How is the Information Used?

Unless specifically directed not to do so by the client, PHI may be disclosed to health care providers within the client's "Circle of Care" who need to know the information in order to provide the appropriate care or treatment. The "Circle of Care" may include other health care professionals outside of this agency, such as psychologist, doctor, nurses, and home service providers who provide health care services to the client.

- Client information is used by agents (employees, consultants, students and volunteers) to provide necessary care or treatment.
- Collaborating and working as part of a multi-disciplinary team to provide services to clients.
- Teaching and fostering a learning environment.
- Quality assurance, and evaluation.
- Accreditation and licensing processes.
- Agency employees are trained and understand that client information is private and can only be used or accessed to provide care and service to carry out our main activities.
- If client information is to be used for any purpose other than our main activities, the agency employee must ask the client for permission.
- If the agency has express consent from a client to use his/her information for research purposes, that information will only be used for research if the strict process in PHIPA is followed by both the Agency and the researcher and the client is not identified by the information.

- Sometimes the law requires the agency to disclose client information, such as to a Children's Aid Society when they are doing an investigation or when the agency learns that a child may be at risk of harm. Information will be disclosed only if the law requires or permits the agency to do so.

Obtaining Consent:

Consent may be implied or express.

Express consent will be obtained when i) disclosing client information to someone who is not a HIC (e.g., school, employer, lawyer, etc.); or ii) disclosing client information to a HIC but for purposes other than providing for health care. Express consent means specific verbal or written authorization for the collection, use or disclosure.

Where the agency is collecting, using or disclosing PHI for health care purposes, the law normally permits the agency to rely on implied consent where the surrounding circumstances allow the agency to make a reasonable determination that the client would agree to the collection, use or disclosure.

A client may withhold or withdraw consent at any time. If it is believed that the withholding or withdrawing of consent may compromise client care, the client will be so advised. The client will also be told if others within the Circle of Care cannot be provided with that information when it is requested. Clients may provide an express written instruction that information not be used or disclosed. Employees of the agency, or the Privacy Officer, will assist any client with this process.

The agency may collect, use or disclose PHI without client consent in limited circumstances that are required or permitted by law.

Consent is only valid when obtained from a "capable" person. To be capable of consenting, the individual must be able to understand the information relevant to the decision and the consequences of giving, withholding or withdrawing consent. If an individual is deemed to be incapable of making decisions about the PHI, the agency will obtain consent from a substitute decision-maker, as determined by law. Agency employees will discuss the implications of giving, withholding or withdrawing consent with the client or substitute decision-maker and will allow opportunity for any questions to be resolved. This process will be noted in the client file.

Retaining and Disposing of PHI:

The agency will retain client information in a secure manner and keep it for as long as necessary to fulfill the purposes for which it was collected, or as required by law. After that, records will be destroyed in a secure manner, such as cross-cut shredding.

Accuracy of PHI:

Agency employees will take all reasonable steps to ensure that information collected is accurate, complete and up-to-date at the time of collection. Information will be routinely updated as it is available to fulfill the purposes for which it is collected. Reasonable steps will be taken to ensure that information disclosed to others under this policy is accurate, complete and up-to-date and will be so indicated at the time of use or disclosure.

Security of PHI:

PHI in the custody of this agency is protected by security measures and safeguards designed to protect client information against loss, theft or unauthorized access, disclosure, copying, use or modification. Some of the steps taken to protect that information include:

a) Physical measures
- Protecting the premises by lock and alarm;
- Locking offices that contain PHI; and,
- Storing PHI in locked filing cabinets.

b) Administrative measures
- Creating and maintaining internal operational procedures regarding security;
- Ensuring that access to PHI is restricted to only those agency employees who need it in order to provide the necessary care or treatment;
- Training agency employees regarding privacy responsibilities;
- Monitoring printers and fax machines to ensure they are kept in secure areas;
- Auditing information and security practices to ensure agency employees compliance with this privacy policy; and,
- Establishing contracts with outside parties to ensure the confidentiality of PHI.

c) Technological measures
- Requiring individualized passwords to access computers;
- Ensuring a high level of security for PHI stored in electronic format; and,
- Ensuring that anti-virus, firewall and security measures are current and implemented on all computers that maintain PHI.

All employees, directors, volunteers, students and other professional staff members are aware of the importance of keeping client information confidential. As a condition of employment or association with this agency, they are all required to sign a Confidentiality Agreement.

Compliance Monitoring and Auditing

Access, use, disclosure and sharing of information will be monitored and all suspected breaches of this Policy will be investigated by the Privacy Officer. Actions to be taken will be determined by the Executive Director and Directors in consultation with Human Resources, Legal Counsel, and/or other Agency stakeholders according to the nature of the breach and parties involved.

Agency operational areas and programs conduct appropriate reviews and audits of their systems and processes to ensure compliance with Agency policies and standards.

Responding to Breach of Policy

Staff will report any real or suspected breaches of this Policy in connection with any Agency program or activity immediately upon becoming aware. All reports must be made to the Privacy Officer or delegate. Staff may report real or suspected breaches without any fear of reprisal.

All incidents involving theft or loss of information will be promptly addressed for containment, investigation, reporting, and remedial actions.

If an Agency staff identifies, or has reason to believe, that information has been lost or stolen or has been accessed by unauthorized person(s), that staff member will notify the Privacy Officer or delegate immediately either verbally or by e-mail. The notification will be followed by a written submission that includes all pertinent details leading to this assertion. The Privacy Officer will conduct an investigation and, in consultation with the Executive Director/delegate, will notify the affected client(s) or staff member(s), the I.T. Department (if applicable), the appropriate Ministry, and, as required, the police.

The following steps will be taken by the Privacy Officer or delegate if it is suspected that there has been a privacy breach:

Step 1: Respond immediately by implementing the privacy breach protocol

- Ensure appropriate staff are immediately notified of the breach, including the workers whose clients are potentially affected by the privacy breach.
- Address the priorities of containment and notification as set out in the following steps.

Step 2: Containment – Identify the scope of the potential breach and take steps to contain it

- Retrieve the hard copies of any information that has been disclosed.
- Ensure that no copies of information have been made or retained by the individual who was not authorized to receive the information and obtain the person's contact information in the event that follow-up is required.
- Determine whether the privacy breach would allow unauthorized access to any other information (e.g. an electronic information system) and take whatever necessary steps are appropriate (e.g. change passwords, identification numbers and/or temporarily shut down a system).

- Consider notifying the Information and Privacy Commissioner/Ontario ("IPC/O") and/or legal counsel if appropriate.
- If inappropriate access has been identified, staff who may have breached privacy will be placed on a paid leave of absence during the investigation and access to the client database will be disabled.

Step 3: Notification – Identify those individuals whose privacy was breached and notify them of the breach.

- At the first reasonable opportunity, any affected clients (or others whose information has been affected) will be notified.
- The type of notification will be determined based on the circumstances (such as the sensitivity of the information, the number of people affected, and the potential effect the notification will have on the client(s)).
    - For example, notification may be by telephone or in writing, or in limited circumstances, a notation made in the client's file to be discussed at their next appointment (such as if there is risk of harm or if there is no other means to communicate with the client).
- Provide details of the extent of the breach and the specifics of the information at issue.
- Advise affected clients of the steps that have been or will be taken to address the breach, both immediate and long-term.
- Consider engaging the IPC/O, legal counsel and the insurer, as appropriate.

Step 4: Investigation and Remediation

- Conduct an internal investigation into the matter. The objectives of the investigation will be to:
    - Ensure the immediate requirement of containment and notification have been addressed.
    - Review the circumstances surrounding the breach.
    - Review the adequacy of existing policies and procedures in protecting information.
    - Address the situation on a systemic basis.
    - Identify opportunities to prevent a similar breach from happening in the future.
- Change practices as necessary.
- Ensure staff are appropriately re-educated and re-trained with respect to compliance with the privacy protection provisions of PHIPA and the circumstances of the breach and the recommendations of how to avoid it in the future.
- Continue notification obligations to affected individuals as appropriate.
- Consider engaging IPC/O, legal counsel and the insurer, as appropriate.
- Consider any disciplinary consequences with staff or contract issues with independent contractors or vendors that follow from the privacy breach.

Client Access to Their Information:

Clients may request access to any records in Yorktown Family Services custody or control that contain information about them by writing to their primary worker or to the agency's Privacy Officer. The client will receive at least a preliminary response from the Privacy Officer within *thirty* days and a full response within *sixty* days.

Right of access to information is not absolute. Access may be denied when:

- Denial of access is required or authorized by law; or,
- The request is frivolous or vexatious or in bad faith.

If access is denied, the Privacy Officer will provide the reason(s) why and will also notify the client of his/her right to complain to the Information Privacy Commissioner of Ontario (IPC). Clients may be charged a reasonable fee (based on cost recovery) for copies of information in the client record. Clients will be advised of any fees before copies are made.

Corrections to PHI:

Depending on the circumstances, clients have the right to request corrections to a record of PHI within this agency's custody or control. Such a request is to be made by providing a written request to the Privacy Officer who will respond to all written requests within thirty days, although in certain circumstances additional time to provide a response may be required. If agreed, every effort will be made to correct the record by recording the correct information and crossing out the incorrect information, without obliterating it. Any changes will be initialled and/or noted by the Privacy Officer. Requests may be denied if:

- are not satisfied that the record is incomplete or inaccurate for the purposes for which the information was recorded;
- The request consists of a record that was not originally created by employees of this agency and this agency does not have sufficient knowledge, expertise or authority to correct the record;
- The request consists of a professional opinion or observation that an employee made in good faith; or,
- The request is frivolous or vexatious or made in bad faith.

Written reasons will be provided for any refusal to correct a client record.

Internal Operational Procedures:

The agency will periodically establish or revise various operational procedures to give effect to this policy. These may include, for example, procedures regarding access or correction requests.

Compliance with this Policy:

All agents of Yorktown Family Services are required to know and comply with this policy. Annual confirmation of compliance is required. Any breach of this policy may result in significant action up to, and including, termination of employment or, in the case of other professionals or organizations, termination of the working agreement. Employees may only use client information as permitted by the agency and within legal limitations. All employees must notify the Privacy Officer at the first reasonable opportunity if client information is lost, stolen or accessed without authorization.

Clients are advised to direct any questions or concerns respecting the information contained in this policy or the agency's privacy practices to the Privacy Officer. Every effort will be made to answer all questions and to promptly investigate any concerns that may be raised regarding this policy or a potential privacy breach. If an issue is found to have merit, all appropriate measures will be taken, including taking disciplinary action or amending these information practices.

Yorktown Family Services - Privacy Officer

Privacy Officer
Yorktown Family Services
300-2010 Eglinton Avenue West
Toronto, Ontario
M6E 2K3

Tel: 416.394.2424 Fax: 416.394.2689

Ontario's Information and Privacy Commissioner

While every effort will be made to provide a resolution to all privacy concerns, clients may also contact the Information and Privacy Commissioner of Ontario at:

Information and Privacy Commissioner
Suite 1400
2 Bloor Street West
Toronto, Ontario M4W 1A8 1.800.387.0073 TTY 416.325.7539