POLICIES AND PROCEDURES

TITLE: Privacy	**POLICY NUMBER:** A-4-250
APPROVED BY: Chief Executive Officer	
DEVELOPED BY: Senior Director, Clinical Operations & Quality Improvement	**DATE:** January 23, 2004 (O), January 10, 2005 (R), November 2008 (R), April 2011 (R), March 2012 (R), May 2019 (R), February 2023 (R)

POLICY:

Cota is obligated to protect the confidentiality of the personal health information of all our service users while providing services. Cota's Privacy Policy ("Policy") is organized around the ten principles of Ontario's Personal Health Information Protection Act (PHIPA) which governs the way personal health information may be collected, used and disclosed.

The information practices of Cota concerning confidential information that is not personal health information, such as the personal information of its workers or business information, are defined in the Cota Confidentiality Policy. If there is a discrepancy between this Policy and PHIPA, PHIPA takes precedence.

Definitions:

"Personal Health Information" (PHI) includes any identifying information verbal, written or electronic about an individual that:

- Relates to the clinical physical or mental health conditions of the individual;
- Relates to any specific health service provided to the individual;
- Is collected in the course of providing health services to the individual;
- Is collected incidentally to the provision of health services to the individual; or
- Identifies the donation by the individual of any body part or any bodily substance of the individual or information derived from the testing or examination of a body part or bodily substance of the individual

Information is identifying when it identifies an individual or when it is reasonably foreseeable in the circumstances that it could be utilized, either alone or with other information, to identify the individual.

"**Health Information Custodian**" (HIC) means an individual or organization identified in section 3 (1) of PHIPA who has custody or control of personal health information. Cota, as an organization, is a HIC.

An "**Agent**" in relation to PHIPA, means any individual who is authorized by the agency to do anything with respect to personal health information.

For Cota it includes: employees, volunteers, students or contracted agents who deal with, or have access to personal health information.

"**Privacy Officer**" Every organization that is a health information custodian must appoint one or more employees as Privacy Officers. A Privacy Officer is responsible for the privacy practices of the organization.

At Cota, a member of the senior management team is the designated Privacy Officer and contact person.

PROCEDURES:

Anyone who collects uses or discloses PHI on Cota's behalf is required to follow these 10 information practices:

1. Accountability

The Chief Executive Officer (CEO) designates a Privacy Officer (PO) to act on their behalf and it is the PO who is responsible for overseeing and implementing the privacy practices. The CEO is the back-up Privacy Officer.

The PO is responsible for:

- Keeping current with legal privacy developments and with best practices within the healthcare industry.
- Addressing privacy questions concerns and challenges to the organization.
- Ensuring continuous improvement of information practices.
- Ensuring that Privacy training is implemented and ongoing for all Agents.
- Receive and respond to complaints as they relate to privacy.

Cota shall make the name and contact information of its PO publicly available through the Cota website, as well as, through notices that are distributed to Cota clients and make this information available upon request.

All Cota agents are responsible for managing the personal health information to which they have access in compliance with this Policy. Cota shall take the necessary steps (e.g., contractual or other means) to ensure that a comparable level of privacy practices is employed by external stakeholders (third parties).

Cota has policies and procedures that give effect to this Policy including:

- Secure Retention, Transmission and Destruction of Personal Health Information;
- Confidentiality Policy;
- Privacy Breach Management Protocol;
- A complaints process to respond to alleged or actual breaches of the Policy (via Occurrence Reporting);
- Procedures for communicating the Policy to Cota agents, for training them about privacy policies and procedures, and a Confidentiality and Privacy agreement that all agents are required to sign as a condition of employment or engagement with the organization, which requires them to read, understand, and comply with the policy.

Cota is to review this Policy and its supporting policies and procedures every two (2) years to ensure its privacy practices adhere to legal requirements and industry best practices. Any amendments to this Policy and its supporting policies and procedures are approved by senior management. Amendments are communicated to Cota employees by Cota's Privacy Officer or designate.

2. Identifying Purposes for Collecting Personal Health Information

Cota and its Agents collect personal health information for the following purposes; direct client care, administration of Cota and the health care system, authorized health research, teaching and statistics, complying with legal and regulatory requirements and planning, delivering, evaluating, monitoring and allocating resources to Cota programs and services.

Cota Agents shall:

- Identify and explain the purpose(s) for which Cota collects, uses, and/or discloses personal health information at or before the time the information is originally collected;
- Communicate verbally or in writing the identified purposes to the person(s) from whom the personal health information is sought;
- Communicate verbally or in writing any new purpose for using or disclosing personal health information and obtain the client's consent, as appropriate, prior to making any such uses or disclosures.

3. Consent for Collection, Use and Disclosure of Personal Health Information

Cota can rely on implied consent with other health care custodians under the law, however when possible and appropriate expressed consent will be obtained. The Client/Substitute Decision Maker may withdraw such consent at any time. Consent to collect use, and release PHI expires when the client is discharged from Cota or when they decide to withdraw consent which is effective from the date of withdrawal and cannot be retroactively applied.

Information which is collected, used, or released will be used only for the purpose for which it is collected.

If expressed consent has been obtained, reasonable attempts must be made to obtain it in writing.

To release **written** information the service provider must always obtain expressed and if possible written consent.

To release information **verbally** to anyone in the circle of care implied consent may be used; however, if possible, consent is preferable. The Client has the right to request a copy of the information that is released. For the release of the health record or any part thereof, the procedures outlined in *Policy A-4-280*, Access to Health Records must be followed.

When a third party wants to speak to a Service Provider about a client who has been discharged from Cota the Service Provider requires the discharged client's signed consent before speaking to the third party.

> A client may at any time withdraw or withhold their consent to the use and/or disclosure of their personal health information for the purposes of health care by giving reasonable notice, verbally or in writing to Cota's service provider of their intention to do so. If the request to withdraw consent is verbal, the client requesting the withdrawal will be asked to follow up with a written request. The client cannot retroactively withdraw consent.

Upon receiving such a request, the service provider will discuss the following with the client

- The potential impact their withdrawal may have on their health care; and
- Any legal limitations to which their withdrawal of consent may be subject (e.g., personal health information will be disclosed in a life-threatening situation regardless of the client's withdrawal of consent)

Where a client has withheld his/her consent to disclose his/her personal health information. Cota will notify any health information custodian to which it discloses that client's personal health information of that fact.

There are circumstances where Cota is permitted or required by law to collect, use and disclose personal health information without the consent of the client, such as health research, teaching and statistics, public health monitoring and quality assurance. In such circumstances, Cota will only use and disclose clients' personal health information without consent as permitted or required by law.

4. Limiting Collection of Personal Information

Cota shall limit the amount and type of personal health information it collects to that which is necessary to fulfill the purpose identified. Cota shall collect personal health information, using fair and lawful means, to ensure that clients are not misled or deceived about the purposes for which their information is collected. Cota shall not collect personal health information indiscriminately or unnecessarily.

5. Limiting Use Disclosure and Retention of Personal Information

Cota and its agents shall not collect, use or disclose clients' personal health information for purposes other than those for which it was collected, except with the consent of the client to whom the personal health information relates or as required by law.

Where consent is obtained to use or disclose personal health information for a new purpose not previously identified, Cota shall document this new purpose in this Policy.

Cota shall retain personal health information only as long as necessary to fulfill the purpose for which it was collected or as required by laws governing retention of personal health information and health records. Personal health information that Cota and its

agents use to make a decision about a client shall be retained long enough to allow the client access to the information after the decision has been made. The types of information Cota routinely collects are contact information, assessment and service delivery information.

Cota has policies and procedures in place to specify retention periods and methods to destroy personal health information once retention periods are complete *(see Policy #A-4-20: Secure Retention, Transmission and Destruction of Confidential Information).* Such processes prevent unauthorized parties from gaining access to personal health information in the course of the destruction process.

6. Accuracy of Personal Information

Cota ensures that personal health information collected is as accurate, complete and up to date as is necessary for the purposes for which it is be used and to minimize the possibility that inappropriate or inaccurate information may be used to make decisions about the client's service delivery.

Cota provides documentation, training and support, and chart review practices.

Where a client successfully demonstrates that personal health information in the custody or control of Cota is inaccurate or incomplete. Cota shall amend the information as is necessary to make it accurate and complete so long as it does not involve making a correction to an opinion made by a service provider in good faith. Where appropriate, the amendment of such personal health information shall be provided to third parties having access to the information in question. Any statement of disagreement shall be attached to the client's record of personal health information. Cota does not amend documentation of other organizations.

7. Safeguards for Personal Information

All personal health information in the custody or under the control of Cota shall be protected by the following administrative, technical, and physical safeguards.

Cota uses administrative safeguards such as this Policy and its supporting policies and procedures, contractual means (e.g., confidentiality agreements and contracts) and training to inform its employees and third parties of the safeguards they must employ to protect the personal health information to which they have access.

- Cota applies technical safeguards such as computer access codes (e.g., logins and passwords) and encryption software on all electronic data stores where personal health information is retained (e.g., USB key or computer hard drives).
- Cota uses physical safeguards such as locked cabinets, offices, and secure work environments to protect personal health information in electronic and hard copy form from inappropriate or unauthorized use and disclosure.
- Cota ensures the transmission of personal health information is limited to secure and/or encrypted methods (e.g., scanning on Cota issued iPhones using only Cota approved apps). One Mail is used, if/when available, to appropriately share PHI between other service providers within a client's circle of care and referral sources.

- Service providers are strictly prohibited from using text message as a means to exchange PHI with clients, internal Cota staff or external service providers.

8. Openness about Cota's Privacy Policy

Information about Cota's privacy and practices are available including:

- Contact information of Privacy Officer
- The process of gaining access to personal health information held by Cota
- A description of the types of personal health information held by Cota, including a general account of its use.
- Copies of any brochures or other information that explain Cota's policies, standards or codes.

Individuals may direct inquiries or complaints related to Cota's management of personal health information and compliance with this Policy to the PO *(Policy #A-6-30: Occurrence Reporting).*

9. Individual Access to Personal Health Information

Upon request in writing to the PO, a client shall be informed of the existence of any personal health information related to him/her in the custody or under the control of Cota and the uses to which that information has been put and disclosure by Cota of such information to any third parties.

A service user seeking access to information about what personal health information Cota has in its custody or under its control, has the responsibility of providing satisfactory proof of identification to Cota for the organization to be able to provide an account of the existence, use and disclosure of personal health information *(Policy #A-3-110: Access to Health Records)*

In providing information about third parties to whom personal health information has been provided, Cota shall be as specific as possible.

Cota may require the client seeking access to his/her information to meet with an appropriate healthcare practitioner about the requested personal health information before such information is provided *(see Policy #A-3-110: Access to Health Records).*

If, for any reason, Cota has personal health information about a client that it cannot release to that client for legal or other reasons, the reasons for such refusal shall be provided to that client upon request. A client is entitled to challenge the refusal by submitting a challenge to the refusal in writing to the PO.

Cota shall provide clients with access to their personal health information at minimal or no cost to the client and within thirty (30) days, subject to extension upon appropriate notice. Should the client require photocopies of such information, Cota reserves the right to charge the client an amount that would reasonably cover the costs associated with the photocopying.

10. Challenging Compliance with Cota's Privacy Policy

An individual is entitled to challenge Cota's compliance with this Policy. Any such challenge must be made in writing and directed to the PO or by email at: privacy@cotainspires.ca

Cota has procedures to receive and respond to complaints, challenges or inquiries about its practices relating to the handling of personal health information.

Anyone who submits a written complaint, challenge or inquiry shall be provided with a written copy of Cota's procedures governing such complaints, challenges and inquiries.

Cota investigates all complaints received in accordance with the established procedure. If a complaint is found to have merit, Cota shall take appropriate measures to address the complaint, including if necessary, amending its policies and practices in respect of the handling of personal health information.

REFERENCES:

A-4-70 – Client Consent to Collect, Use and Release Information Specific to Provision of Services
A-4-20 – Secure Retention, Transmission and Destruction of Personal Health Information
A-6-30 – Occurrence Reporting
A-4-280 – Access to Health Records
A-4-50 – Client Consent to Treatment/Services Policy
Health Care Consent (1996)
Privacy Breach Protocol

PRIVACY BREACH MANAGEMENT PROTOCOL

Privacy Breach Definition:

"Whenever a person has contravened or is about to contravene a provision of the Act or its regulations."

STEP 1	**RESPONDS IMMEDIATELY** • Anyone that is aware of a privacy breach should inform the Privacy Officer within 1 business day. • Depending on the risk to the organization, the Privacy Officer may need to contact the CEO or Manager, Quality & Risk • The reporting staff/manager will complete an Occurrence Report
STEP 2	**CONTAINMENT: Identify scope of the potential breach and take steps to contain it** The Privacy Officer is responsible for: • Ensuring that the organization retrieves any hard copies of any Personal Health Information (PHI) that has been disclosed • Ensuring that no copies of PHI have been made or retained • Determining whether the breach would allow unauthorized access to any other PHI and take whatever steps needed (eg. change passwords, ID numbers)
STEP 3	**NOTIFICATION: Identify those individuals whose privacy was breached and notify them of the breach** • The Privacy Officer is responsible for ensuring that the service user or applicant is notified at the first reasonable opportunity (by phone, in writing, or in person or through other means that has been vetted with legal counsel and Information and Privacy Commissioner and authorized by the CEO) and has been advised of the breach and steps to contain the breach.
STEP 4	**INVESTIGATION/REMEDIATION** The Privacy Officer will: • Conduct an internal investigation: ensure that immediate requirements of containment and notification have been addressed; review circumstances surrounding breach; review internal policies • Report the breach to the IPC (if appropriate) • Ensure that staff have adequate training

For detailed information about protocols, please refer to www.ipc.on.ca
What to do When Faced with a Privacy Breach: Guidelines for the Health Sector