

**Wait Time Information Office
Privacy Policy
Fourth Edition**

Effective Date	September 1, 2006
Last Revision	April 24, 2008
Approved by	Sarah Kramer – Lead – Wait Time Information Strategy Pamela Spencer – Chief Privacy Officer, Cancer Care Ontario

Introduction

Purpose

The Wait Time Information Office (WTIO) Privacy Policy ("Policy") is structured around the ten fair information practice principles of the Canadian Standard Association's *Model Code for the Protection of Personal Information*¹ and applies to personal health information collected, used, disclosed and retained by the WTIO for the purpose of managing and operating the Wait Time Information System (WTIS), ensuring data quality and data protection, performing data audits, and analyzing and reporting data.

This Policy identifies related documents and relevant authorities for each of the fair information practices, where appropriate.

Background

In November 2004, the Ontario Ministry of Health and Long-Term Care (the "Ministry") launched a provincial Wait Time Strategy. The strategy provides Ontario patients with greater access to health care services by enabling the monitoring, management, and reduction of wait times for surgical procedures and treatments and is a fundamental part of the Ministry's overall initiative to transform and improve the province's health care system.

One of the primary objectives of the Ontario Wait Time Strategy was to create a central reporting system to track, measure, and reduce wait times in key service areas. To this end, the Ontario Wait Time Strategy implemented a web-based information system - the WTIS - to facilitate wait times management and provide the public with wait time information.²

The Ministry designated Cancer Care Ontario ("CCO") to operate and manage the WTIS. In order to fulfill this role, CCO conducted a privacy impact assessment (PIA) on the WTIS which analyzed privacy risks and made corresponding recommendations regarding CCO's collection, use, and disclosure of personal health information via the WTIS. CCO implemented the recommendations made in the PIA, which included the development and adoption of this Policy.

¹ The Canadian Standards Association's *Model Code for the Protection of Personal Information* (Q830) sets out ten principles that balance the privacy rights of individuals and the information requirements of private organizations.

² Sarah Kramer, Ontario Wait Time Information System, December 6, 2005.

Privacy Policy

Principle 1 - Accountability

An organization is responsible for personal information under its control and shall designate an individual or individuals who are accountable for the organization's compliance with the following principles.

The Ontario Ministry of Health and Long-Term Care (the "Ministry") designated Cancer Care Ontario ("CCO") to operate and manage the Wait Time Information System (WTIS) pursuant to CCO's status as a *prescribed entity* under the Ontario *Personal Health Information Protection Act, 2004* (PHIPA) until the WTIS is transitioned to a permanent data custodian.³ CCO established the Wait Time Information Office (WTIO), which is responsible for managing the operations of the WTIS, ensuring data quality and data protection, performing data audits, and analyzing and reporting data.

The Lead - Wait Time Information Management Strategy (WTIMS) (and CCO's Vice President and Chief Information Officer) and CCO's Chief Privacy Officer (CPO) appointed a WTIO Privacy Lead who is responsible for the day-to-day operation of privacy processes within the WTIO and compliance with this Policy.⁴ The WTIO Privacy Lead reports jointly to the Lead - WTIMS and the CCO CPO on the privacy responsibilities described in the *WTIO Privacy Lead Terms of Reference*.⁵ The Lead - WTIMS and the CCO CPO are ultimately responsible for the privacy practices of the WTIO.⁶

This Policy and its supporting procedures are reviewed annually or when changes are made to legislation that governs the WTIO to ensure that it continues to adhere to legislative requirements and privacy best practices. The Policy review is conducted jointly by the Lead - WTIMS and the CCO CPO or their delegate(s). This Policy, and any amendments to the Policy, are approved by the Lead - WTIMS and the CCO CPO and communicated to WTIO staff⁷ by the WTIO Privacy Lead.⁸

If there is a discrepancy between this Policy and PHIPA, PHIPA takes precedence.

This Policy applies to the WTIO so long as CCO is mandated by the Ministry to manage the WTIS.

The WTIO relies on CCO's Information Technology (IT) Department to support the WTIS application, which CCO licenses to participating hospitals. The CCO IT Department provides IT services such as servers, a data centre, computer support, and disaster recovery for the WTIS.⁹ The CCO IT Director is responsible for ensuring personal health information managed via these

³ Letter to the Information and Privacy Commissioner/Ontario from Cancer Care Ontario, October, 2006.

⁴ Wait Time Information Office Privacy Lead – Terms of Reference, February 25, 2008.

⁵ Cancer Care Ontario Privacy Delegation Chart, November 1, 2007.

⁶ The Wait Time Information Office adhered to Cancer Care Ontario's existing policies and procedures that were in place until this Policy and its supporting procedures were approved.

⁷ For the purposes of this Policy, Wait Time Information Office staff include all employees, students, contractors or third parties who are employed or affiliated with Cancer Care Ontario to support the Wait Time Information Office and Wait Time Information System.

⁸ Wait Time Information Office Compliance Procedure, February 25, 2008.

⁹ Cancer Care Ontario is subject to specific privacy requirements as a "service provider" (described in section 6(1) of the *Personal Health Information Protection Act, 2004* [PHIPA] Regulation) that licenses the WTIS to participating hospitals.

services is secure and managed in compliance with CCO IT security policies.¹⁰ The Systems Security Specialist is responsible for day-to-day operation of IT security processes within CCO.

The WTIO is located within CCO's offices. Therefore, CCO's Facilities Department is responsible for the physical security of the WTIO such as staff identification and door access.

Principle 2 - Identifying Purposes

The purposes for which personal information is collected shall be identified by the organization at or before the time the information is collected.

The WTIO collects personal health information for the purposes of:

- enabling health care providers and their staff to collect information about wait times;
- reporting wait times to physicians, patients, and the public;
- providing hospital administrators and physicians with the information they require to manage wait lists and to make informed decisions; and
- enabling health care providers to review patients currently on a wait list in order to identify priorities for scheduling procedures.

The WTIS does not directly support surgical or procedure booking/scheduling functionalities. In addition, the WTIO does not use personal health information from the WTIS to contact individuals for any reason.

The WTIO Privacy Lead is responsible for training WTIO staff about this Policy, including the purposes for which the WTIO collects, uses, discloses, and retains personal health information in relation to the WTIS as well as the safeguards used to protect personal health information in the WTIO's custody and control.¹¹

Principle 3 - Consent

The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate.

Health care providers (i.e. health information custodians) are permitted to disclose wait time data about individuals, without their consent, to the WTIO for the purpose of the WTIS in accordance with CCO's authority as a "prescribed entity" under PHIPA. As such, patients do not have the right to opt out of the WTIS for wait time reporting and wait list management purposes.¹²

It is the responsibility of the health care provider to ensure the requisite consent requirements are satisfied when personal health information is collected via the WTIS. For example, health care providers must provide a notice of their information practices to patients that describe the purposes for which the WTIS collects patient information from health care providers and how such information will be subsequently used or disclosed. The WTIO makes this Policy available to health care providers for use in their notices as appropriate. As a privacy "best practice", the WTIO also makes available a public written statement of information practices describing the purposes of the WTIO's collection, use, and disclosure of personal health information.

Principle 4 - Limiting Collection of Personal Health Information

¹⁰ See Acceptable Use of Cancer Care Ontario Systems, June 10, 2005, Cancer Care Ontario Remote Access and Wireless Network Policy, June 10, 2005, Cancer Care Ontario Data Center Access and Usage Policy, March 2005, Cancer Care Ontario Security of Electronic Information Policy, January 29, 2007, Cancer Care Ontario Media Destruction Policy and Procedure, June 2005.

¹¹ Wait Time Information Office Privacy Training and Awareness Procedure, February 25, 2008.

¹² Ontario *Personal Health Information Protection Act, 2004*, s. 45(1).

The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means.

The WTIO is committed to only collecting the minimum amount of personal health information required to report on wait times in order to assist health care providers in managing wait lists. The WTIS only collects the following information about patients who are waiting for diagnostic procedures or surgeries:

- Patient identifying information: patient name, patient demographic data (e.g. address, postal code, date-of-birth) and patient identifiers (e.g. health card number, medical record number);
- Health care provider information: physician information and referring physician information (e.g. health care provider number, health care provider name, demographic data, provider specialty);
- Facility information: hospital or other facility information and type of facility;
- Surgical wait time information: the procedure for which the patient is on a wait list (e.g. surgical procedure type, date of decision to treat, original scheduled procedure date, rescheduled date (where applicable), actual procedure date); and
- Prioritization information: based on priority tools for each clinical area, specific clinical parameters and a priority level score.

The physicians leading wait time clinical expert panels are responsible for reviewing the data elements collected by the WTIS to ensure they satisfy this principle.¹³ A privacy impact assessment (PIA) will be conducted on all new or amended collections of personal health information via the WTIS. The Lead – WTIMS and the CCO CPO will authorize or reject new collections of data based on the analysis of the PIA.

Principle 5 - Limiting Use, Disclosure and Retention of Personal Health Information

Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal information shall be retained only as long as necessary for the fulfillment of those purposes.

The WTIO only uses and discloses personal health information it receives to calculate wait time statistics and to develop and apply clinical parameters to facilitate wait list management.¹⁴

A PIA will be conducted on all new or amended uses and/or disclosures of personal health information via the WTIS. The Lead – WTIMS and the CCO CPO will authorize or reject new uses or disclosures as well as retention plans of data based on the analysis of the PIA.

Limiting Use

Use of the WTIS by WTIO staff is limited to those who require access to perform their job functions (e.g. calculating wait times or supporting the WTIS). The WTIO Privacy Lead ensures WTIS users understand their responsibilities to protect the personal health information to which they have access via the WTIS before access to the WTIS is permitted.

The WTIS Data Steward is responsible for authorizing WTIO staff's use of the WTIS, and confirming that such access is still appropriate and has only been used for the staff's job responsibility.¹⁵

¹³ Sarah Kramer, Phase II Steering Committee, July 14, 2006.

¹⁴ Ontario Regulation 329/04 Amended to O. Reg. 322/07, made under the *Personal Health Information Protection Act, 2004*, s.18.

The WTIS is also accessed by users at participating health care organizations. These users must be authorized by their organization and must read and accept an acceptable use agreement¹⁶ before access to the WTIS is permitted. Participating health care organizations are responsible for ensuring their users comply with the acceptable use agreement and their requirements under PHIPA. In order to monitor WTIS user activities, participating hospitals may request a copy of audit logs describing their users' activities or the activities of WTIO staff supporting the WTIS by contacting the WTIO Privacy Lead.¹⁷

Limiting Disclosure

The WTIO discloses personal health information from the WTIS and via reports to the health care provider who originally disclosed it to the WTIO. The WTIO does not release additional identifiers through the WTIS or in these reports.¹⁸

The WTIS discloses patient identifiers to the Ministry to enable the Ministry to accurately identify and organize records of personal health information that relate to a patient in the provincial Enterprise Master Patient Index.¹⁹

The WTIO may disclose personal health information from the WTIS to researchers for research studies approved by a Research Ethics Board that meet the requirements outlined in PHIPA. The researcher must submit an application in writing to CCO and enter into an agreement with CCO stipulating restrictions on the use, security, disclosure, return or disposal of the information. The CCO Data Access Committee approves the disclosure.²⁰

The WTIO may also disclose personal health information from the WTIS to:

- another prescribed registry for facilitating and improving the provision of health care;
- a prescribed entity for the management, evaluation, monitoring or planning of the health system;
- a health data institute for analysis of the health system;
- a governmental institution of Ontario or Canada.²¹

The WTIO releases aggregate information publicly to the Ministry and Local Health Integration Networks.²²

¹⁵ Wait Time Information Office Direct Access Procedure, February 25, 2008.

¹⁶ Wait Time Information System End User License Agreement.

¹⁷ Wait Time Information Office Direct Access Procedure, February 25, 2008.

¹⁸ Ontario Regulation 329/04 Amended to O. Reg. 322/07, made under the *Personal Health Information Protection Act, 2004*, s.18(5).

¹⁹ Ontario Regulation 329/04 Amended to O. Reg. 322/07, made under the *Personal Health Information Protection Act, 2004*, s.18(8).

²⁰ Ontario *Personal Health Information Protection Act, 2004*, s. 44(1)-(6) and Ontario Regulation 329/04 Amended to O. Reg. 322/07, made under the *Personal Health Information Protection Act, 2004*, s.15-17.

²¹ Ontario Regulation 329/04 Amended to O. Reg. 322/07, made under the *Personal Health Information Protection Act, 2004*, s.18.

²² As part of the Wait Time Information Office (WTIO) Data Analytics Program, the WTIO will offer standardized wait times reports to hospitals, the Ministry of Health and Long-Term Care, and Local Health Integration Networks via a business intelligence tool, iPort Access. iPort Access will form the foundation of a Wait Times Data Warehouse.

The WTIS Data Steward reviews all aggregate and de-identified data disclosures for residual risk of identification before the information is released. The WTIO Privacy Lead is consulted to determine if a risk of identification may exist.²³

Limiting Retention

The WTIO retains personal health information in the WTIS indefinitely and in the least identifying form possible to allow the WTIO to analyze wait times.

WTIO staff are responsible for shredding WTIS data retained outside the WTIS and in paper form when it is no longer required to support a function of the WTIO. WTIO staff are responsible for physically destroying WTIS data retained outside the system in soft-copy (e.g. compact disk) or sending the portable media to the CCO IT Director, who is responsible for disposing of it in accordance with CCO's media disposal policies.²⁴

Principle 6 - Accuracy

Personal information shall be as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used.

It is not the current practice for the WTIO to update "source" records (i.e. those received from participating health care organizations). Health care providers are required to take reasonable steps to ensure that the personal health information they submit about their patients is as accurate, complete and up-to-date as is necessary for wait time reporting and wait list management purposes.²⁵ The WTIS includes functionality to assist health care providers in meeting this requirement (e.g. mandatory field checks). The WTIO Data Quality Program also provides tools to assist hospitals in identifying and correcting data errors, as well as conducting data quality reviews on a monthly basis of all data submitted to the WTIS.

The WTIO Privacy Lead will refer requests from individuals to correct their information in the WTIS to the health care provider who submitted the personal health information so that the individual may follow up with the health care provider directly to correct information in the "source" system.²⁶

Principle 7 - Safeguarding Personal Health Information

Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.

The WTIO employs administrative, technical, and physical safeguards to protect personal health information in its custody and control against loss or theft, as well as unauthorized access, disclosure, copying, use or modification. These safeguards apply to personal health information in paper or electronic form, and personal health information in storage or in transit.

Administrative Safeguards

The WTIO uses this Policy and its supporting procedures, contractual means (including confidentiality agreements and contracts), and training to inform WTIO staff of the safeguards they must employ to protect the personal health information to which they have access via the WTIS. The WTIO Privacy Lead is responsible for ensuring all WTIO staff have undergone training

²³ Cancer Care Ontario Data Disclosure Procedures, March 5, 2007.

²⁴ Cancer Care Ontario Media Destruction Policy and Procedure, June 2005.

²⁵ Ontario *Personal Health Information Protection Act, 2004*, s. 11(2)(a).

²⁶ Wait Time Information Office Access and Correction Procedure, February 25, 2008.

on this Policy and have confirmed their understanding of this Policy by signing a privacy acknowledgement form.²⁷

It is the responsibility of the WTIO Director to ensure a CCO confidentiality agreement is signed when the WTIO staff person begins his or her employment with the WTIO. The WTIO Privacy Lead also reviews the confidentiality obligations of WTIO staff with them upon leaving their positions with the WTIO.

A PIA and threat-risk assessment (TRA) will be conducted on all new or amended services provided by the WTIO to participating hospitals. The Lead – WTIMS and CCO CPO will authorize or reject new services based on the analysis of the PIA and TRA.

CCO also enters into written agreements with all hospitals it provides services to, which set out the terms and conditions under which services are provided and hospitals may use those services.

Physical Safeguards

CCO provides a secure physical environment for the WTIO and the equipment on which personal health information is retained. The WTIO Privacy Lead reviews the physical security safeguards on a regular basis to ensure that they adequately protect personal health information used by the WTIO and assists CCO in implementing physical safeguards that are required as a result of the review.²⁸

Technical Safeguards

The WTIO relies on the technical safeguards in place within CCO's IT Department to protect IT services that support the WTIS. CCO applies industry standards and tests its systems to ensure that personal health information and the equipment and communication systems are secure.²⁹

WTIO staff are responsible for following CCO policies related to IT and facilities security, and employing all safeguards provided by CCO to protect data in the WTIS. The IT Director is responsible for informing WTIO staff of those policies through training and awareness.

Principle 8 - Openness about Privacy Practices

An organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information.

The WTIO makes information about its privacy practices and the collection, use, and disclosure of personal health information via the WTIS available to WTIO staff, the general public, and participating health care providers.³⁰ This information includes:

- general information on the WTIO's privacy practices;
- a description of data the WTIS collects and retains;
- a description of the safeguards in place to protect data retained in the WTIS; and
- contact information of the WTIO's Privacy Lead.

The WTIO makes this information available:

- on the CCO website (www.cancercare.on.ca);

²⁷ Wait Time Information Office Privacy Training and Awareness Procedure, February 25, 2008.

²⁸ Wait Time Information Office Compliance Procedure, February 25, 2008.

²⁹ Principles and Policies for the Protection of Personal Health Information at Cancer Care Ontario, May 2005.

- on the Ontario Wait Time website (www.ontariowaittimes.com);
- through brochures and privacy communications materials the WTIO provides hospitals participating in the WTIS, which hospitals in turn make available to patients and their families;³¹ and
- upon request to the WTIO Privacy Lead.

As a privacy “best practice”, the WTIO also makes a summary of the findings of its PIAs and TRAs available to hospitals participating in the WTIS once a PIA and TRA is completed or when significant changes to the PIA or TRA are made.

All WTIO staff immediately direct enquires for information about WTIO’s privacy practices to the WTIO Privacy Lead. The WTIO Privacy Lead is responsible for responding to the individuals, under the direction of the Lead – WTIMS and the CCO CPO.³²

Principle 9 - Individual Access

Upon request, an individual shall be informed of the existence, use, and disclosure of his or her personal information and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.

Under PHIPA, the WTIO is not obliged to grant individuals’ requests to access or correct their records of personal health information.³³ However, as a privacy “best practice”, when the WTIO receives access or correction requests, the WTIO Privacy Lead provides individuals with the contact information of the health care provider(s) who submitted their personal health information so that individuals may submit their requests directly to the specific health care provider(s).³⁴

Principle 10 - Challenging Compliance

An individual shall be able to address a challenge concerning compliance with the above principles to the designated individual or individuals accountable for the organization's compliance.

An individual may challenge compliance with this Policy by submitting his or her concern or complaint regarding the WTIO’s information practices to the WTIO Privacy Lead at wtioprivacy@cancercare.on.ca or in writing to the WTIO Privacy Lead, Cancer Care Ontario, 505 University Avenue, 17th Floor, Toronto, Ontario, M5G 1X3.

The WTIO Privacy Lead reviews all concerns and complaints in accordance with applicable procedures.³⁵ If a complaint is found to be justified, the WTIO Privacy Lead will conduct an investigation and take appropriate measures including, if necessary, amending its policies and procedures.

Individuals may also make a complaint to the Information and Privacy Commissioner/Ontario.

³¹ See Wait Time Information Office Privacy Brochure, Wait Time Information System Frequently Asked Questions for Hospital Administrators, Patients, Privacy Officers, and Physicians, and Wait Time Information System Overview.

³² Wait Time Information Office Inquiries and Complaints Procedure, February 25, 2008.

³³ Ontario *Personal Health Information Protection Act, 2004*, s. 51(1)(d).

³⁴ Wait Time Information Office Access and Correction Procedure, February 25, 2008.

³⁵ Wait Time Information Office Inquiries and Complaints Procedures, February 25, 2008.

References

The following documents must be followed to implement the Wait Time Information Office (WTIO) Privacy Policy ("Policy"):

- Wait Time Information Office, Privacy Lead Terms of Reference, April 24, 2008.
- Wait Time Information Office, Access and Correction Procedure, April 24, 2008.
- Wait Time Information Office, Compliance Procedure, April 24, 2008.
- Wait Time Information Office, Direct Access Procedure, April 24, 2008.
- Wait Time Information Office, Inquiries and Complaints Procedure, April 24, 2008.
- Wait Time Information Office, Privacy Breach Management Procedure, April 24, 2008.
- Wait Time Information Office, Privacy Training and Awareness Procedure, April 24, 2008.
- Wait Time Information Office, Data Disclosure Procedures, March 5, 2007.
- Cancer Care Ontario, Privacy Governance Chart, April 2008.
- Cancer Care Ontario, Acceptable Use of Cancer Care Ontario Systems, April 18, 2008.
- Cancer Care Ontario, Data Center Access and Usage Policy, April 18, 2008.
- Cancer Care Ontario, Media Destruction Policy and Procedure, April 23, 2008.
- Cancer Care Ontario, Remote Access and Wireless Network Policy, April 18, 2008.
- Cancer Care Ontario, Security of Electronic Information Policy, February 19, 2007.

The following documents inform the Policy:

- Letter to the Information and Privacy Commissioner/Ontario from Cancer Care Ontario, October 2006.
- Principles and Policies for the Protection of Personal Health Information at Cancer Care Ontario (Third Edition), April 2008.
- Ontario *Personal Health Information Protection Act, 2004* and its Regulations
- Wait Time Information System, Privacy Impact Assessment, February 25, 2008.
- Wait Time Information System, License Agreement.
- Wait Time Information System, End User License Agreement.
- Canadian Standards Association's *Model Code for the Protection of Personal Information*.