Privacy in a Telemedicine Environment

OTN Reference Manual for Health Care Professionals
About this Guide

In Ontario, the *Personal Health Information Protection Act, 2004* (PHIPA) governs the collection, use, and disclosure of personal health information, such as patient’s names, diagnoses, and conditions, which may be shared over video or teleconference.

OTN created this reference manual to describe the privacy practices that OTN and its members must follow to ensure personal health information is protected in an environment where this responsibility is shared. This guide showcases privacy lessons that OTN and its member have learned over the past four years. We are confident that these “lesson learned” will help guide your privacy practices as you schedule, organize, facilitate, assist with and conduct telemedicine across the province.

**Note:** The information in this guide is not meant to replace any policies, information, training or educational opportunities at your own facility or organization.

Learning Objectives:

- Understand why privacy is so important in a telemedicine environment
- Understand the roles of OTN and its members as health information custodians (HIC), agents and health information network providers (HINP)
- Learn how to safeguard a telemedicine studio in compliance with PHIPA and OTN guidelines
- Identify privacy incidents in a telemedicine environment and apply “lessons learned” to prevent incidents
- Understand the steps involved in reporting and handling privacy breaches
## Table of Contents

- Why is Privacy Important in a Telemedicine Environment? .................................................. 4
- Privacy at OTN and Overview – Roles and Responsibilities under PHIPA .......................... 5
- Privacy in a telemedicine environment – Your Responsibilities .......................................... 8
- OTN Privacy Resources ........................................................................................................ 9
- Getting Ready for a Telemedicine Session ............................................................................ 10
- Privacy during a Telemedicine Session .................................................................................. 12
- Privacy after the Telemedicine Session .................................................................................. 14
- Policies, Procedures and Guidelines ....................................................................................... 15
- Lessons Learned .................................................................................................................... 16
- Who to Contact with Privacy Concerns .................................................................................. 22
Let’s Talk Privacy

Thousands of Clinical Consultations in Ontario are Conducted Using Telemedicine.

Why is Privacy Important? Four Reasons....

1. In no other field is trust more critical than in the health care sector. **Some of our most sensitive information is shared with our health care provider.**

2. Generally, a patient sees his or her health care provider “in person”, in an environment where her or she knows the room or office in which he or she is consulted is secure and private. However, in a clinical telemedicine consultation, **patients must trust that their consulting clinicians as well as the telemedicine technology (e.g. video conferencing system) will provide the same degree of privacy and security.** Therefore, OTN and its members **all** have a role in protecting the privacy of personal health information transmitted using telemedicine services.

3. If patients do not have confidence that their personal health information, including their image, will be protected, they may withhold information or choose **not participate** in a telemedicine appointment.

4. In Ontario, the collection, use, disclosure, retention and disposal of personal health information by health care providers and organizations is governed by the **Personal Health Information Protection Act, 2004** and it’s Regulation. **It is important that OTN, health information custodians, recipients and electronic service providers understand and follow their requirements under the legislation.**
Privacy at OTN - An Overview

This section serves to assist members in understanding the privacy statutory responsibilities that OTN has for personal health information or for the services it provides to enable members to manage personal health information in a telemedicine environment. This section also includes the resources that members may reference to learn more about how OTN fulfills its responsibilities.

**OTN’s Responsibilities under PHIPA**
Under PHIPA, OTN is subject to privacy requirements as a ‘health information network provider’, an ‘agent’ and as a ‘service provider’.

**OTN as a Health Information Network Provider**
OTN acts as a ‘health information network provider’ when it provides telemedicine services to two or more of its members; enabling those members to disclose personal health information to one another through videoconference, teleconference and network services or applications, such as the Store and Forward Solution.¹

**As a HINP, OTN has the following obligations:**

1. **Notify** If PHI is lost, or accessed or disclosed inappropriately by OTN while scheduling, organizing, facilitating and/or or conducting a telemedicine event, OTN’s Privacy Office will notify the applicable health information custodians, members and/or partners of this privacy breach.

---

¹ *Personal Health Information Protection Act, 2004 – O. Reg. 329/04 s.6 (3)*
Created by: Sylvie Gaskin
Date of Creation: December 2008
Version: 1
© OTN 2009
2. **Provide** the public and members with a written description of OTN’s services and policies and safeguards to protect personal health information. This information is currently available on OTN’s website.

3. **Make available** to health information custodians an audit log of all OTN’s accesses to or transfers of personal health information via OTN’s telemedicine technology or supporting applications.

4. **Conduct** privacy impact assessments (PIA) and threat and risk assessments (TRA) on services that may affect the privacy of individuals who are the subject of the information, and provide a summary of these assessments to every applicable health information custodian. OTN conducts PIAs and TRAs when new technologies and/or its services involve PHI and provides written summaries to the applicable health information custodian(s).

5. **Ensure** the third parties OTN retains to assist in providing its telemedicine services (e.g. data management, technical support) agree to comply with OTN’s HINP requirements.

6. **Enter** into written agreements with each health information custodian and third party. OTN executes membership and third party agreements.

In addition, OTN makes publicly-available privacy contact information and responds to privacy inquiries and complaints. For example, OTN has communication material on its website that includes contact information for the Privacy Office, studio posters and patient information pamphlets.

**OTN as an Agent**

When OTN receives and handles PHI on behalf of health information custodians (HICs) to facilitate scheduling and referral management, OTN is subject to privacy requirements as an ‘agent’² under PHIPA. PHI including a patient’s name, contact information, health card number, attending physician, and reason for referral is necessary to arrange telemedicine consultations with a health care professionals.

Under PHIPA, ‘agents’ obligations flow from the responsibilities of the health information custodians upon whose behalf the agent is collecting, using, and disclosing personal health information. Typically, this means that agents follow custodians’ policies or procedures (e.g. nurses who collect, use, or disclose PHI in the course of their duties at a hospital follow the hospital’s privacy policy). However, in the case of OTN, it has developed a **Privacy Program** and executed a **Membership Agreement** that allows it to meet its obligations as an agent of several custodians in a “global” manner.

---

² *Personal Health Information Protection Act, 2004*, s.17

Created by: Sylvie Gaskin
Date of Creation: December 2008
Version: 1
© OTN 2009
OTN as a Service Provider

OTN acts as a “service provider” when it supplies its services for the purpose of enabling a health information custodian to use electronic means to collect, use, modify, disclose, retain or dispose of personal health information.\(^3\)

As a service provider, OTN has the following obligations:

1. **Only use** personal health information to which it has access if necessary in the course of providing its services.

2. **Never disclose** any personal health information to which it has access in the course of providing the services.

3. **Ensure** employees or any person acting on OTN’s behalf agree to comply with OTN’s service provider requirements.

OTN Privacy Structure

In order to fulfill its requirements under PHIPA, OTN has put in place a comprehensive privacy structure, which includes:

- A privacy and security governance and operational structure
- Specialized privacy and security staff
- A Privacy and Security Lateral Team
- Policies, procedures and guidelines which inform OTN staff, consultants, students, contract workers and member sites about the network and OTN’s privacy/security practices
- Training material for staff, consultant, students and contract workers

Facts about OTN’s Chief Privacy Officer, information practices, access, correction and/or complaint processes are available on OTN’s website [www.otn.ca](http://www.otn.ca) on the Privacy Best Practice Toolkit page.

---

\(^3\) *Personal Health Information Protection Act, 2004* – O. Reg. 329/04 s.6 (1)

Created by: Sylvie Gaskin

Date of Creation: December 2008

Version: 1

© OTN 2009
Privacy in a telemedicine environment– Your responsibilities

The protection of personal health information in a networked environment is a shared responsibility. This responsibility is shared between those using the network and OTN. Member sites using the network, which are health information custodians, are responsible for the following:

• Designating a contact person (Chief Privacy Officer) for the purposes of the Act

• Establishing & maintaining information practices

• Identifying the purposes for which PHI is collected, used and disclosed and obtain consent

• Making available a written statement on:
  ✓ Information practices
  ✓ Contact person’s contact information
  ✓ Access, correction, inquiry & complaint procedures

• Taking reasonable steps to ensure personal health information is accurate, complete and up-to-date

• Notifying patients if use or disclosure of PHI is beyond what is described in written statement

• Complying with legislative requirements outlined in PHIPA

• Training staff, & physicians acting on your behalf how to follow your information practices about PHIPA requirements

• Being familiar with OTN privacy & security policies, procedures and guidelines

• Taking reasonable steps to protect personal health information when arranging for, conducting & following-up with clinical telemedicine activities

• Reporting telemedicine-related privacy breaches to OTN
OTN Privacy Resources
OTN has developed several communication tools, policies and guidelines, including this ‘Reference Manual’ to assist OTN, its members and partners in complying with the provisions in PHIPA and with privacy ‘best practices’ in a telemedicine environment.

OTN Web-Site
The OTN web-site ‘Privacy Best Practice Toolkit’ page holds privacy fact sheets and information for patients and health care professionals as well as relevant policies, forms, pamphlets, posters and guidelines.

OTN Communication Material
OTN has developed notices and patient information brochures to assist member sites and health care professionals in providing patients with relevant information about a telemedicine session. These are also available on the ‘Privacy Best Practice Toolkit’ page.

OTN Training
OTN employees, contracted workers and students are introduced to Privacy at OTN through the OTN Orientation Program. OTN has developed an e-training program for OTN member sites engaging in administrative, educational and clinical activity which includes privacy learning objects.

OTN Learning Opportunities
You will also find privacy specific learning content in our member facing newsletters and learning modules.
Getting ready for a Clinical Telemedicine Session

Privacy Tip #1

The steps taken to protect personal health information during a telemedicine session should be similar to those used for a face-to-face consultation. These steps include the following:

- When you have telemedicine personnel who are not regulated health care professionals (e.g. information technology personnel), it is important that these individuals have a thorough understanding of and a respect for the importance of confidentiality and privacy in a telemedicine environment. Make this guide available to them.

- Assure patients/parents that information shared during telemedicine sessions will be kept confidential and that the session is only seen and heard by the individuals located in the telemedicine room.

- OTN’s Patient Information Brochure includes important information for patients about how OTN uses and protects their personal health information. Make this brochure available to patients and their families.
Privacy Tip #2

When faxing a referral containing personal health information to OTN schedulers please follow the best practices highlighted in 'OTN Facsimile Transmission Member Guidelines'.

Below are some points to consider from the Guideline:

- Maintain frequently used numbers on a master list and check it regularly for accuracy.
- When programming facsimile (fax) numbers on a master list, check the number carefully.
- Check fax numbers for accuracy on the display screen and against the master list.
- When possible, call the intended recipient prior to faxing to ensure he or she is ready to receive the fax.
- Use a cover sheet with the following detailed information:
  - Name, address and phone number of the sender;
  - Number of pages being faxed; and
  - A statement that the information is confidential and may be subject to PHIPA.
- If you are notified that a fax you have sent was transmitted in error to an incorrect location, alert your immediate supervisor, Privacy Officer and/or risk manager (per your facilities policy or practice).
- If a fax related to OTN (e.g. a telemedicine referral form) is transmitted in error to an incorrect location, notify the OTN Chief Privacy Officer at privacy@otn.ca.

Privacy Tip #3

Do not email personal health information. It is not a good practice.
Privacy during a Clinical Telemedicine Session

Privacy Tip #1

Place a sign outside the door to indicate that a telemedicine session is underway. The sign should read ‘Videoconference in Progress, Please Do Not Disturb’.

Privacy Tip #2

No patient information should be discussed outside the room where the telemedicine session will occur and no information should be discussed inside that room before the door to that room is closed.

Privacy Tip #3

Only the telemedicine personnel and individuals involved in the care of the patient should attend the telemedicine session.

Privacy Tip #4

The patient site and the consultant site should pan the camera around the room where the telemedicine session will take place to assure participants that only those in the room are participating. Both sites should introduce everyone present.
Privacy Tip #5

• Patients and consultants must be informed of and give their consent to have anyone else attend the telemedicine session.

• Permission to include observers during the telemedicine session must be obtained from the patient and the consulting health care professional prior to the telemedicine session.

• The patient, consultant and/or the telemedicine personnel have the right to refuse any request for someone else to observe a telemedicine session.
Privacy after the Telemedicine Session

Privacy Tip #1

Make sure the room is locked and access is limited to authorized individuals only.

Privacy Tip #2

If the telemedicine platform is situated in a multipurpose room and privacy is required, make sure the telemedicine platform is turned off when the room is being used for purposes other than telemedicine.

Privacy Tip #3

The “Mic-Off” feature should be enabled. Keep the camera focused on a view that will not compromise privacy (e.g. pointed to an empty wall). A camera preset can be established for this purpose. Secure the remote control in a locked cabinet or in a location with limited access.

For more information please see 'Guideline for Physical Privacy of Patients during a Telemedicine Session'
Privacy Policies, Procedures and Guidelines
OTN has developed a number of relevant policies, procedures and guidelines to assist individuals organizing and participating in telemedicine sessions. To learn more about the documents listed below please click on the Privacy Best Practice Toolkit or go to www.otn.ca

OTN Privacy Policy
Guidelines for Physical Privacy of Patients during Telemedicine Sessions
Guidelines for Endpoint Security
Facsimile Transmission Member Site Guidelines
Consent to Record a Telemedicine Session Policy Guidelines
Consent Form to Record a Telemedicine Session
Accessing Personal Health Information Request Policy and Procedure
Correcting Personal Health Information Policy and Procedure
Privacy Complaint Policy and Procedure
Privacy Incidents and Lessons Learned

Even in a perfectly planned telemedicine session, things can go wrong. We need to work together to contain incidents, notify the appropriate parties when things go wrong, and look for opportunities to improve our processes. The following ‘Privacy Facts’ were developed based on lessons learned in a telemedicine environment and created to help prevent privacy breaches.
Privacy Fact #1:

Avoid Connecting Before the Scheduled Time

Many OTN sites have multi-purpose rooms for videoconferencing. From time to time, individuals conducting a clinic or a clinical session may connect prior to the scheduled time. In doing so, the clinic or clinical session may begin before the patient is ready or during a session that is running late, or the wrong patient may be in the multi-purpose room. This means that individuals may inappropriately view the patient or his or her personal health information.

How to Prevent this Privacy Breach

- Point the camera to a wall (using presets) between sessions as soon as the previous call is disconnected.
- At the patient site focus the camera on the nurse or Telemedicine Coordinator only (who is in the room with the patient) until the patient is introduced.

See the OTN’s Guidelines for End Point Security for more information.
Privacy Fact #2:

Even When Your Telemedicine System Does Not Appear To Be In Use, You Could Be Connected

Many OTN sites use one room for clinical, educational and administrative events. Even when the videoconferencing system may not appear to be connected, you could be on camera if your system is set to ‘auto-answer-on’. This could lead to a privacy breach if you are with a patient and another site inadvertently connects to your system or it could lead to an embarrassing moment if you are on screen without your knowledge.

How to Prevent this Privacy Potential Privacy Breach

- Ensure that you have the auto-answer “off” or “auto-answer point-to-point no” enabled
- When not in use, a videoconference system used for clinical or confidential events located in a multipurpose room should be turned off and/or unplugged.
- Keep the camera pointed to a place in the room where a person will not be in view.
- Snapshot and remote video streaming settings should be left disabled because both features could allow an unauthorized person to monitor a clinical or confidential session.

See the [OTN’s Guideline for Physical Privacy of Patients during a Telemedicine Session](#) for more information.
Privacy Fact #3:

Misdirected Faxes May Lead To a Privacy Breach

If you send a fax to the wrong location, the personal information contained in the fax may be inadvertently disclosed to unauthorized individuals. If you send a fax to the correct location, but the fax is picked up by an unauthorized individual, patient’s personal health information may also be inappropriately accessed.

When sending information by fax, employ the following practices to protect personal health information:

- Consider whether sending confidential information via fax is the most appropriate means of communication. For example, sending the information via courier or secure file transfer may be more secure.
- Use a fax cover sheet with a privacy notice, description of the documents and total number of pages the recipient should expect to receive.
- Use a fax machine located in a protected area, so that individuals cannot easily access faxed documents.
- Double check the fax number you have for the recipient to ensure it is correct.
- Double check your documents before you send your fax to ensure only the correct information is faxed to the recipient.
- Check the documents you receive by fax to ensure you have all the pages that were sent.
- Before pressing “send”, verify in the fax machine’s display window that you have keyed the fax number correctly.
- When possible/practical, call the recipient of the fax prior to sending the fax to notify him or her that a fax is about to be sent.
- If you discover that a fax you have sent containing confidential information has been transmitted to an incorrect location, try to retrieve the fax and/or to ensure that the recipient destroys it.
- If you receive a fax in error, contact the sender as soon as possible to confirm whether or not the fax should be returned or destroyed.

See the OTN’s Facsimile Transmission Members Guidelines for further information.
Privacy Fact #4:

Connecting in Error to a Site or Telemedicine Event Impacts Patient Privacy and Your Organization’s Reputation

Personal health information may be inadvertently transmitted/accessed when a site erroneously connects to the wrong site or telemedicine event. When this happens, the site may inadvertently view a patient whose telemedicine session is in progress.

How to Prevent this Privacy Breach

- If you have connected in error to another site and/or session, disconnect immediately.
- If a remote site has connected to your site or session in error, ask the site to disconnect immediately or disconnect the site, if you can.
- If the site is not disconnecting, contact OTN’s Service Desk (1-866-454-6861) immediately.

Who to contact when connected in error to a telemedicine event

- Contact OTN’s Chief Privacy Officer at privacy@otn.ca immediately so that OTN can help you review systems and processes and identify opportunities to prevent this from happening in the future.
- Contact your organization’s Privacy Officer to trigger patient notification requirements, if required, and to review systems and processes and identify opportunities for improvement.
Privacy Fact #5:

A Lack of Physical Privacy of Patients Can Lead to a Privacy Breach

It is important to locate telemedicine rooms in areas that provide optimal physical privacy and to take reasonable steps to protect patient’s physical privacy when conducting telemedicine consultations. This will prevent privacy incidents that may occur when telemedicine consultations are inadvertently interrupted or overheard due to lack of physical safeguards.

How to Prevent this Privacy Breach

• Locate telemedicine rooms in a low traffic area.
• Choose rooms with window coverings that you can close (e.g. blinds).
• If possible, select a room that is soundproof.
• Provide a private area inside the room that the patient may use to change his or her clothes.
• Prepare and place a sign outside the door when a telemedicine session is under way.
• Lock the door during the videoconference session to prevent an unplanned interruption.

See the Guideline for Physical Privacy of Patients During a Telemedicine Session for more information.
Privacy Questions or Concerns? Call us or contact us at:
1-866-454-6861 or privacy@otn.ca
Legend

Email/Website Information

To learn more

Tips/Best Practice

Contact Us

Important Information