ONTARIO TELEMEDICINE NETWORK

Privacy Policy Framework

Prepared with assistance from

June 2015

Document Control

The electronic version of this document is recognized as the only valid version.

DOCUMENT IDENTIFIER AND LOCATION:	
Review Frequency:	This document will be reviewed at least once every three years
Document Prime*	*Enquiries relating to this document should be referred to the responsible Document Prime.

Approval History

APPROVER(S)	TITLE	APPROVED DATE
Pal Gill	Vice-President Finance and Administration	April 2014
Privacy & Security Lateral Team	Privacy & Security Lateral Team	March 2014

Revision History

VERSION NO.	VERSION DATE	SUMMARY OF CHANGE	CHANGED BY
V.1	20 December 2013	Initial draft	Excela Associates
V.2	10 February 2014	Revisions, post January 2014 review by privacy team.	Excela Associates
V.3	13 March 2014	Revisions based on review of Action Register Items	Excela Associates
V.4	10 June 2015	Updated with approved edits	Henry Bury

Table of Contents

1 PREAMBLE

1.1 GLOSSARY

1.1.1 Definitions

(See section-specific definitions, where necessary, in the relevant policy sections.)

TERM	DEFINITION
Asset	Any tangible or intangible information, hardware, software, or service that has value to the OTN. It includes a major application (e.g. MS Outlook), general support system (e.g. SAP), high impact program (e.g. Service Desk), physical plant (e.g. Off-site data centre), mission critical system (e.g. TSM/NCompass), personnel (e.g. employees), equipment (e.g. computer), or a logically related group of systems (e.g. Portal).
Confidential Information	Any information given or used in confidence that may be disclosed only to authorized individuals on a need-to-know basis or information that is consolidated for regulatory purposes such as legal proceedings. This also includes information related to business operations such as employee agreements, financial or business records, and contracts
Health Information Custodian (HIC)	"Health information custodian", subject to subsections (3) to (11) of PHIPA, means a person or organization described in PHIPA who has custody or control of personal health information as a result of performing the person's or organization's powers or duties. (See PHIPA for a complete definition.)
Health Information Network Provider (HINP)	PHIPA defines a health information network provider as a person who supplies goods and services to two or more health information custodians that enable the custodians to collect, use, modify, disclose, retain or dispose of personal health information electronically, if certain requirements are met. Health information network providers must: Notify the custodian of any breaches; • Perform risk and privacy assessments; • Provide an audit trail; • Ensure that third parties comply with the restrictions on the use and disclosure of personal health information; • Enter into an agreement with the custodian; and • Make publicly available information about the provider's services to the custodian.
Incident Category	OTN defines 4 categories of privacy incidents: • No Breach - No PHI, PI or confidential information has been breached. • Breach - PHI, PI or confidential information has been breached according to PHIPA, PIPEDA or OTN policy. • Near Miss - There was potential for a breach however no breach occurred.

Mobile/Portable/Removable device	Refers to a computing device that may be carried on or with the person, typically having a display screen with touch input and/or a miniature keyboard, e.g., smartphone or tablet, or that may be easily carried or moved, and that can be operated by self-contained batteries while in transit, e.g., laptop. Removable storage devices are used to transport or store computing data, e.g., USB stick, USB Hard drive, CD-R, DVD-R.
Personal Health Information (PHI)	Identifying information about an individual in oral or recorded form, if the information as referenced in Personal Health Information Protection Act, 2004 (PHIPA or Act): • Relates to the physical or mental health of the individual, including information that consists of the health history of the individual's family; • Relates to the providing of health care to the individual, including the identification of a person as a provider of health care to the individual; • Is a plan of service within the meaning of the Home Care and Community Services Act 1994, for the individual; • Relates to the donation by the individual of any body part of bodily substance of the individual or is derived from the testing or examination of any such body part or bodily substance; • Is the individual's heath number; or, • Identifies an individual's substitute decision maker.
Personal Information (PI):	Personal information includes PHI and any factual or subjective information, recorded or not, about an identifiable individual. This includes information in any form, such as: • age, name, ID numbers, income, ethnic origin, or blood type; • opinions, evaluations, comments, social status, or disciplinary actions; and • employee files, credit records, loan records, medical records, existence of a dispute between a consumer and a merchant, intentions (for example, to acquire goods or services, or change jobs) Personal information does not include the name, title or business address or telephone number of an employee of an organization.
Privacy Breach	A privacy breach may take the following forms: • The collection, use, and disclosure of personal health information that is not in compliance with the Act or its regulation; • A contravention of the privacy policies, procedures or practices implemented by a prescribed person; • A contravention of agreements involving Personal Information /Personal Health Information including Third Party Service Providers retained by OTN; and • Circumstances where personal health information is stolen, lost or subject to unauthorized use of disclosure or where records of personal health information are subject to unauthorized copying modification, or disposal.
Privacy Team	The privacy team and their contact information are detailed on OTN's Intranet and the internet at www.otn.ca. The privacy team can be contacted through privacy@otn.ca. Privacy breaches that are assigned or are assessed at a high or critical severity level will be reviewed acknowledged and acted on immediately or as soon as reasonably possible.

Personal Health Information Protection Act, 2004 (PHIPA or Act)	Ontario legislation governing OTN's collection, use and/or disclosure of personal information / personal health information.
Risk Ratings	The risk ratings listed below apply to all PHI. There are four levels of severity. It should be noted that where PHI is breached the risk is rated as High by default. All privacy incidents that are reported via our customer care center/service desk are rated as High for escalation purposes to the privacy team. The incidents are then investigated and rated based on the severity of the incident. The risk categories listed below apply to all confidential information including PHI and PI. **Critical -** When a situation occurs that results in non-compliance with PHIPA and/or its Regulation, or with other applicable legislation and/or OTN policy and the result is serious harm to: • *multiple* patients or groups (psychological, reputation), • OTN's reputation or the member site's reputation, • regulatory or contractual liability, • customer loyalty • OTN's position in actual or potential litigation In these instances, PHI is potentially seen and heard for long periods of time by multiple individuals. The individual involved is fully aware of the breach and is upset from this experience. **High -** When a situation occurs that results in non-compliance with PHIPA and/or its Regulation, with other applicable legislation and/or OTN policy and has the potential to or result in serious harm to • a patient or group of patients (psychological, reputation), • OTN's reputation and/or the member site's reputation, • regulatory or contractual liability, • Customer loyalty. In these instances, PHI is potentially seen and heard. The individual involved is fully aware of the breach. **Medium** - When a situation occurs that results in non-compliance with PHIPA and/or its Regulation, with other applicable legislation and/or OTN policy and has the potential to or resulted in moderate harm to • a patient or group of patients (psychological, reputation), • OTN's reputation and/or a member site's reputation, • customer loyalty. In these instances, PHI is seen and heard. The individual involved may or may not be aware of the breach. **Low** - When a situation occurs that results in non-compliance with *PHIPA* and/or its Regulation, with other applicable legislation and/or OTN policy but likely had little or no impact on the patient, OTN or the member site. In these instances, PHI is only seen, and the individual involved is not aware of the breach at the time.

Secure disposal	To remove, destroy or rid of material in a manner that is free from risk of loss, interception and reconstruction.
Severity Level	Any privacy breach involving Personal Health Information is, by default, has a High severity level.
Social Networking	Any collaborative exchange of information via assets such as blogs, email, instant messaging, social network services, wikis, social bookmarking and other instances.
Trojan horse	A computer program that is apparently useful but contains hidden functionality that permits system security mechanisms to be circumvented.
Virus	A type of computer program that can corrupt a computer's hard drive, files, and programs in memory, and that replicates itself to other computers.

1.1.2 Terminology

The following keywords, when used in this policy, have the following meanings.

TERM	DEFINITION
Confidential Information	(See Information Classification Policy for a more robust definition.) This classification applies to information protected by federal (e.g. PIPEDA) and /or provincial (e.g. PHIPA) regulations or policies. Information generally considered private is included in this classification. This classification applies to information that has significant business value and applies strictly for use within the OTN. Its unauthorized disclosure could seriously and adversely impact the OTN, its providers, patients, and employees and its business partners. Examples include corporate Information, personnel Information, PHI, and proprietary information.
Correspondence	All references to correspondence mean communication in a manner that creates a record of such communication, such as a paper memo or e-mail. Communication that does not create a persistent record, such as face-to-face oral communication, does not satisfy requirements for correspondence.
Designate/Delegate	Designates and Delegates are descriptors for managers and/or staff that have, through written authorization, assumed accountability for tasks detailed in this Policy Document. Protocol dictates that appropriate communication ensures that target audiences are informed of the identity and contact information for designates and delegates as well as their privacy-related accountabilities and responsibilities.
May	Means that an item is truly optional. (Often there is a practice to do something, however it is not a requirement.)
Must	Means that the action is an absolute requirement.

Must Not	Means that the definition is an absolute prohibition.
Should, Will	Means that valid reasons may exist in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course.
Should Not, Will Not	Means that valid reasons may exist in particular circumstances when the particular behavior is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing any behavior described with this label.

1.2 REFERENCES

1.2.1 External Documents

- Personal Health Information Protection Act (PHIPA) of Ontario and Ontario Regulation 329/04
- ISO/IEC 27002:2005 "Code of Practice for Information Security Management"
- ISO/IEC 27799 "Health Informatics-Information Security Management in Health Using ISO/IES 27002"
- Information and Privacy Commissioner Ontario Order HO-004

1.2.2 Related OTN Policies

The following OTN policies are often relevant for privacy protection and the IPC' best practice guidelines identify these policies as necessary for a Privacy Policy Framework.

SUBJECT	NUMBER/LOCATION
Acceptable Use of Information Technology Assets Policy	21.05.P
Confidentiality Policy and Procedure	5.05.PP
Enterprise Risk Management Policy & Procedure	17.05.P
Information Classification Policy	21.40.P
Information Ownership Policy	21.41.P
Social Media Policy	10.80.P
SECURITY POLICIES	
Security Governance and Accountability Framework	Corporate Security
Physical Security	Corporate Security
Security Training and Awareness	Corporate Security
Authorization and Ownership of Technology Assets	Corporate Security
Acceptable Use of Technology Assets	Corporate Security
Unacceptable Use of Technology Assets	Corporate Security

Use of Email	Corporate Security
Use of Internet and Intranet	Corporate Security
Mobile Computing and Storage Devices	Corporate Security
Passwords	Corporate Security
Security Audits	Corporate Security
Patch Management	Corporate Security
Change Management	Corporate Security
System Control Audit Logs	Corporate Security
Backup and Recovery	Corporate Security
Business Continuity and Disaster Recovery Plan	Corporate Security

1.3 COMPLIANCE

OTN individuals must be compliant with this policy and its procedures. Violations will include all breaches of confidentiality of OTN information. Compliance will be audited in accordance with and as per the frequency outlined in the Policy and Procedures in Respect of a Privacy Audit.

1.3.1 Violations

OTN individuals must notify the Manager, Privacy and Risk (or designate) and/or the Information Security Officer at the first reasonable opportunity, in accordance with Policy and Procedures for Privacy Breach Management and Policy Information Security Incident Response, if he/she breaches or believes there may have been a breach of this policy or its procedures. The Manager, Privacy and Risk (or designate) and the Information Security Office must notify the each other of potential breaches and incidents that come to their attention.

Issues of non-compliance will be dealt with on an individual basis by the appropriate authority within OTN. Employees who willingly and deliberately violate this policy will be subject to disciplinary action up to and including termination of employment or contract and depending on the circumstances, OTN may seek legal recourse through civil courts.

1.3.2 Exceptions

Under rare circumstances, there may be exceptions to some of the policies in this document. All such exceptions must be approved in advance, by correspondence, by the Director, Privacy/CPO, as appropriate. Any exception that does not have prior written approval will be considered a violation.

2 GOVERNANCE AND ACCOUNTABILITY PRIVACY FRAMEWORK

2.1 PURPOSE

To ensure that OTN has a privacy governance and accountability framework in place in order to comply with the Personal Health Information Protection Act, 2004 and its regulations, as well as with OTN's privacy policies and procedures.

The Framework has been developed with reference to the IPC's Manual for the Review and Approval of Prescribed Persons and Prescribed Entities1 for consistency with the privacy standard expressed therein, although the OTN is not a prescribed entity under PHIPA.

2.2 POLICY

The Chief Executive Officer of OTN is accountable for ensuring that OTN and its agents comply with:

- The Personal Health Information Protection Act, 2004 and its regulations.
- OTN privacy policies and procedures.

The Chief Executive Officer of OTN has delegated overall responsibility for privacy to the Director, Privacy/CPO.

The Director has responsibility for the overall function of the privacy program, planning and strategy, as well as supporting the senior leadership team in implementing various initiatives and services. The Director is counted on to identify privacy risks and opportunities. The Director delegates day-to-day responsibility to the Manager, Privacy and Risk. The Director is a member of the Senior Leadership Team.

Manager, Privacy and Risk has management responsibilities for the implementation of privacy policies and procedures of OTN, as well as the day-to-day management of privacy activities at OTN.

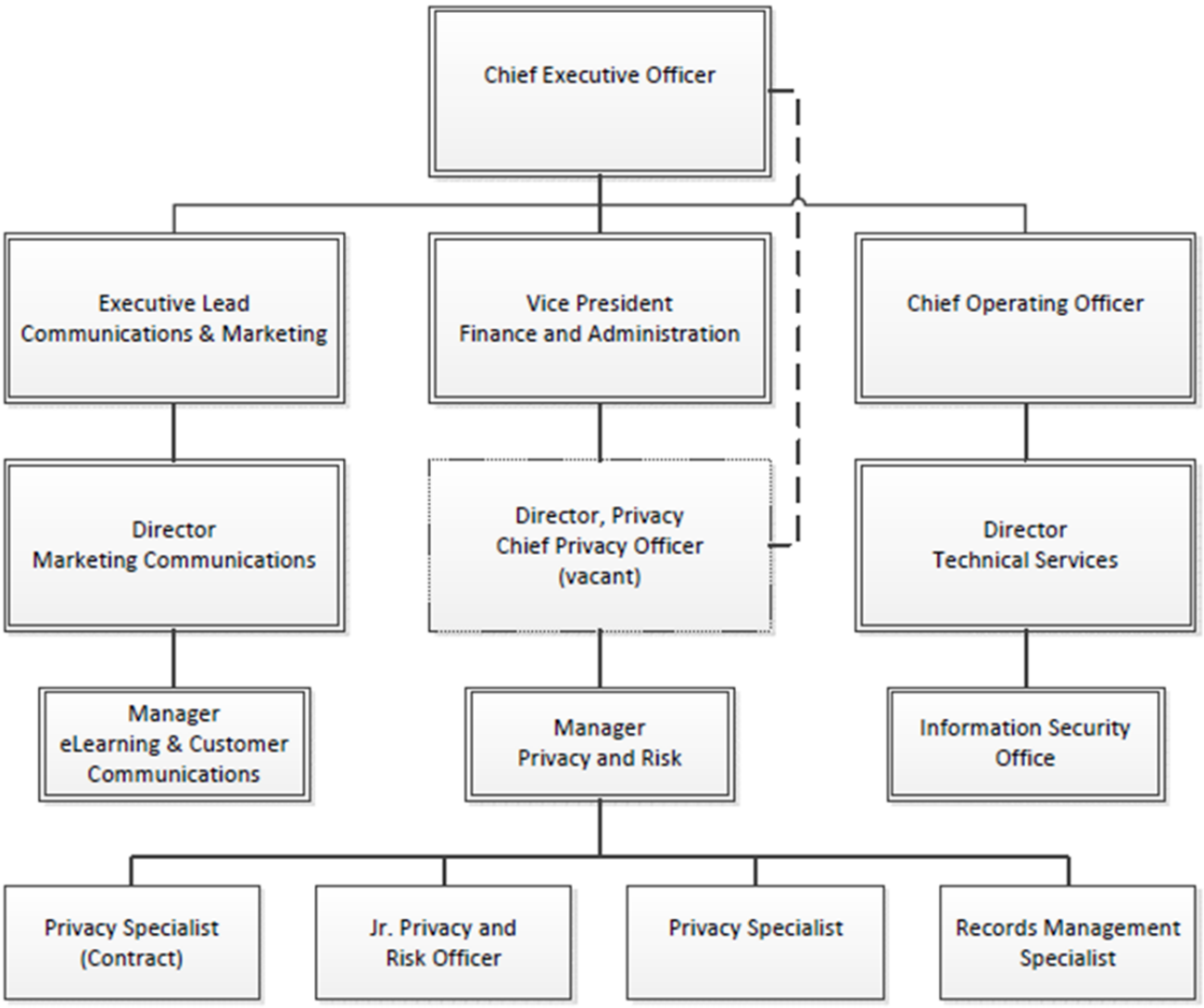
The Manager, Privacy and Risk has staff members to whom specific obligations may be assigned. In carrying out the day-to-day responsibilities of the OTN privacy program, the Manager, Privacy and Risk is supported by the OTN Privacy and Security Lateral Team (PSLT) and the Senior Leadership Team (see Terms of Reference for PSLT attached).

The V-P Finance & Administration has administrative responsibility for the Director Privacy/CPO.

[1] *Manual for the Review and Approval of Prescribed Persons and Prescribed Entities,* Information and Privacy Commissioner of Ontario, 2010, http://www.ipc.on.ca/images/Findings/process.pdf.

2.3 ACCOUNTABILITY GOVERNANCE STRUCTURE

OTN's governance structure as follows:



2.4 PROCEDURES

The Manager, Privacy and Risk (or designate) develops a quarterly privacy report for the Director, Privacy/CPO. The Director finalizes the quarterly report in discussion with the V-P Finance & Administration. The quarterly reports are to form the basis of the content and format of the OTN Annual Report on Privacy Compliance and Strategy prepared for the Chief Executive Officer.

The content of the Annual Report includes:

- A description of privacy training provided for staff.
- Results of privacy impact assessments and privacy audits, their recommendations and the status of implementation.

- Privacy inquiries and complaints and their resolution.
- Privacy breaches, if any, related recommendations and the status of their implementation.
- Annual review of privacy policies and recommendations for change.
- Summary of the bi-monthly Corporate score card provided to the Privacy and Security Lateral Team.
- Privacy Accountability Framework and privacy-focused organization chart (and any proposed changes).
- Privacy Office's Strategic Plan Priorities, Implementation Time-lines, Resource Requirements.

The Annual Report on Privacy Compliance and Strategy is reviewed by the Privacy and Security Lateral Team and reviewed and approved by the Senior Leadership Team and forwarded to the Chief Executive Officer of OTN, who provides the Annual Report to the OTN Board of Directors.

The Manager, Privacy and Risk (or designate) works with Communications to post components of the Annual Report on the OTN VPN site.

The Manager, Privacy and Risk (or designate) ensures that the OTN accountability framework, as well as the organization chart, is included in OTN privacy training.

The Manager, Privacy and Risk (or designate) provides a bi-monthly scorecard to the Director, Privacy/CPO for presentation to PSLT and that scorecard is incorporated in the OTN Governance Scorecard for the Board of Directors.

3 JOB ACCOUNTABILITIES FOR DELEGATED PRIVACY AND SECURITY POSITIONS

At OTN the role of Chief Privacy Officer is held by the Director, Privacy/CPO, who reports to the V-P Finance and Administration and has a 'dotted line' reporting relationship with the CEO of OTN, thus ensuring adequate focus on the strategic nature of privacy management. The Privacy Director/CPO has executive responsibility for Privacy and is accountable to the CEO.

The V-P, Finance & Administration, has limited involvement in managing privacy protections within OTN, but provides administrative supervision to the Director, Privacy/CPO. The following identify the points of accountability for privacy.

3.1 V-P FINANCE AND ADMINISTRATION

The V-P Finance and Administration's Job Accountabilities has the following components listed as key responsibilities and obligations for privacy for OTN, to be undertaken in compliance with relevant OTN policies and procedures:

- Provide Executive oversight and guidance to his/her direct report: Director, Privacy/CPO.
- Provide Executive review for any materials, strategies, issues prior to engaging the CEO, Senior Executives as identified by the Privacy Director/CPO.
- Hold management responsibility for the Director, Privacy/CPO.
- With the V-P Technology & Innovation review and approve and changes to OTN privacy and security training.

3.2 DIRECTOR, PRIVACY/CHIEF PRIVACY OFFICER (CPO)

OTN also has identified the Director, Privacy/CPO reporting to the V-P Finance and Administration as well as having a dotted line reporting relationship to the CEO. The Director has the following key responsibilities and obligations, to be undertaken in compliance with relevant OTN policies and procedures:

- Oversight on the development, implementation, review and amendment of privacy policies, practices, procedures, SOPs, standards and guidelines [together, referred to as policy instruments].
- Ensure compliance with privacy policies and procedures.
- Advise senior executives and CEO of privacy risks, issues and opportunities.
- Provide to the V-P Finance and Administration and CEO the necessary support of the privacy program and facilitate the following:
    - Ensure that privacy policy instruments are transparent, accessible and understood.
    - Facilitate compliance with PHIPA and its regulations.
    - Ensure staff, agents, vendors, consultants, service providers are aware of PHIPA and its Regulation and their duties, obligations and responsibilities in relation to PHIPA.
    - Direct, deliver or ensure the delivery of the initial privacy orientation and the ongoing privacy training and fostering a culture of privacy.
    - Ensure consistent application of sanctions for willful failure to comply with privacy policies and PHIPA for OTN's workforce, extended workforce, and business partners in coordination with Human Resources and legal counsel.
    - Determine needs for system-wide and project-specific PIAs.
    - Oversee the management of privacy complaints.
    - Oversee the management of privacy inquiries.

  - Provide direction for managing privacy breaches or suspected privacy breaches.
  - Determine needs for privacy audits and program reviews.
  - Identify trends, both positive and negative, in privacy management within OTN.
- Liaise with the Office of the Information and Privacy Commissioner regarding PHIPA compliance.

3.3 MANAGER, PRIVACY AND RISK

OTN also has identified the Manager, Risk & Privacy, reporting to the V-P Finance and Administration, as having the following key responsibilities and obligations, to be undertaken in compliance with relevant OTN policies and procedures:

- Periodically review, monitor, assess, investigate and report on OTN systems and projects regarding their compliance with PHIPA and OTN privacy policy and procedures.
- Develop compliance contingency plans in consultation with departments and project teams when compliance to PHIPA or OTN privacy policies and procedures cannot be effectively achieved.
- Oversee and report on privacy training and its uptake in the OTN's work force.
- Coordinate with legal counsel to review and monitor third agent privacy agreements, internal staff confidentiality agreements, information notices, legal practices and requirements under PHIPA.
- Serve as OTN's liaison with the Office of the Information and Privacy Commissioner regarding PHIPA compliance.
- Oversee and report on privacy training and uptake in the OTN's work force.
- Coordinate findings and mitigation or escalation strategies through Risk Management Office/Committee of OTN.
- Review all system-related information security plans to ensure alignment between security and privacy practices and where alignment cannot be reached, escalate to V-P Finance and Administration and CEO.

3.4 CORPORATE SECURITY OFFICER (CSO)

The Corporate Security Officer (CSO) at OTN has been delegated the day-to-day responsibility and authority to manage the OTN security program. The CSO reports directly V-P Innovation & Information Technology through to the CEO. The following conveys responsibilities in line with best practices set out by the IPC.

The Job Accountabilities identifies the key responsibilities and obligations for the role and includes the following obligations, to be undertaken in compliance with relevant OTN policies and procedures:

- Develop, implement, review and amend security policies, practices, procedures, SOPs, standards and guidelines [policy instruments].
- Ensure compliance with the security policy instruments implemented.
- Ensure staff, vendors, consultants and agent service providers are aware of ICES security policy instruments and are appropriately informed of their duties, obligations and responsibilities in relation to PHIPA.
- Provide support to Human Resources' management of securing signed and up to date confidentiality agreements.
- Provide detailed security orientations to staff, vendors, consultants and agent service providers, depending on the requirements of the position the agent has been hired to undertake.
- Implement OTN's confidentiality policies and procedures.
- Direct, deliver or ensure the delivery of the initial security orientation and the ongoing security training and fostering a culture of information security awareness.
- Receive, document, track investigate and remediate information security breaches or suspected information security breaches.
- Conduct security audits.

4 ONGOING REVIEW OF PRIVACY POLICIES AND PROCEDURES

4.1 PURPOSE

To ensure that OTN has in place an effective policy to enable ongoing review of its privacy policies and procedures.

4.2 POLICY

OTN undertakes a review of its privacy policies and procedures on an annual basis or more frequently if required. The purpose of the review is to determine whether amendments are needed or whether new policies and procedures are required to ensure that OTN meets or exceeds industry standards and best practices.

4.3 PROCEDURES

The Manager, Privacy and Risk, at the direction of the Director, Privacy/CPO initiates a review of privacy policies and procedures:

- Annually, or:
  - When a serious breach has occurred in which personal health information in the control and custody of OTN has been lost, stolen, or disclosed without proper authorization.
  - When an Order, Fact Sheet, Guideline and/or best practice is issued by Ontario's Office of the Information and Privacy Commissioner.
  - When amendments are made to the Personal Health information Protection Act, 2004 and its regulation that are relevant to OTN.

In undertaking the review, the Manager, Privacy and Risk (or designate) considers:

- Concerns raised by OTN agents, application service providers and health information custodians.
- Recommendations arising from complaints and inquiries.
- Recommendations arising from privacy audits and investigations into privacy breaches.
- Recommendations arising from privacy impact assessment s.
- Orders, guidelines, fact sheets and best practices issued by the Information and Privacy Commissioner.
- Relevant amendments to the Personal Health Information Protection Act, 2004 and its regulation.
- Evolving industry standards and best practices.
- Inconsistencies between privacy policies and actual practice.

Recommendations for change are forwarded to the OTN Privacy and Security Lateral Team and the OTN Senior Leadership Team for review and approval.

When approval has been obtained, the Director, Privacy/CPO:

- Sends a memorandum to all senior management and staff outlining the changes to policies and procedures, reminding them of the requirement to comply and that compliance will be monitored and enforced by the Manager, Privacy and Risk.
- Distributes relevant information on changes to policies or procedures to service providers.
- Revises training materials.
- Amends existing agreements to reflect changes.

The Manager, Privacy and Risk (or designate) ensures that the annual review process and development of amendments or changes is completed within three months and that communication of changes is completed within a further one-month period.

5 TRANSPARENCY OF PRIVACY POLICIES AND PROCEDURES

5.1 PURPOSE

To ensure that OTN's privacy policies and procedures are transparent for the public and health care providers.

5.2 POLICY

OTN makes readily available to individuals a written public statement about its policies and practices relating to the management of personal health information.

Contact information for designated privacy staff in OTN's privacy team will be published on the OTN's website and made available to members of the public through Telehealth coordinators at referring and consulting sites.

OTN's privacy policy is posted on the OTN's website. It is also available to members of the public on request to OTN's Privacy Office or the Telehealth coordinator at the referring site.

OTN's description of services and safeguards taken to protect personal health information will be posted on OTN's website and is also available to members of the public on request to OTN's Privacy Officer or Telehealth coordinator at the referring site.

OTN makes available it privacy policies through its website at www.OTN.ca. A printed brochure is also available upon request.

5.3 PROCEDURE

The Director, Privacy/CPO (or designate) provides information to the public and health care providers on OTN policies and procedures in language that is clear and non-technical.

The Director, Privacy/CPO (or designate) ensures that the information on the website at www.OTN.ca and in brochures includes:

- A description of OTN privacy policies.
- Frequently asked questions related to OTN privacy policies and procedures.
- A general description of personal health information retained by OTN.
- Summaries of privacy impact assessment s conducted by OTN.
- Name, title, mailing address and contact information of the privacy officer to whom inquiries, concerns or complaints regarding privacy compliance may be directed.

The Manager, Privacy and Risk (or designate) will ensure that brochures or frequently asked questions include the following:

- A description of the policies and procedures implemented in respect of personal health information.
- Types of personal health information collected.
- Health information custodian from whom this information is typically collected.
- The purpose for which personal health information is collected.

- The purposes for which personal health information is used and/or disclosed and the persons or organizations to which the information is disclosed.
- Administrative, technical and physical safeguards implemented to protect the information against theft, loss, and unauthorized use, disclosure, copying, modification or disposal.
- Name, title, mailing address and contact information of the designated staff on the privacy team to whom inquiries, concerns or complaints regarding privacy compliance may be directed.
- Instructions for making complaints are posted on OTN's web site and may be obtained through staff in OTN's privacy office or Telehealth coordinator[2].

Note: information will not be made public if it is reasonable to conclude that doing so would affect the security of the OTN system or the personal health information contained therein.
Updates to public and stakeholder materials are addressed as per OTN Policy on Ongoing Review of Privacy Policies in section 3.

[2] Note: Internal and external privacy inquiries and complaints can be directed to the designated staff in OTN's Privacy Office. Individuals can also contact the office of the Information and Privacy Commissioner of Ontario directly.

6 PRIVACY INQUIRIES

6.1 PURPOSE

The Ontario Telemedicine Network (OTN) is committed to promptly addressing any inquiry relating to the management and protection of its data holdings, to OTN's privacy policies, procedures and practices, or to OTN's compliance with the Personal Health Information Protection Act, 2004 (PHIPA) and its regulation.

6.2 SCOPE

This policy applies to all OTN employees and those with whom OTN has a contract to provide goods or services, who are involved in receiving, documenting, tracking, or responding to a privacy inquiry relating to OTN's privacy policies, procedures and practices or compliance with PHIPA and its regulation.

6.3 POLICY

Anyone may make an inquiry about OTN's privacy policies, procedures and practices or an inquiry related to OTN's compliance with PHIPA and its regulation.

OTN employees and those with whom OTN has a contract to provide goods or services must be compliant with this policy and its procedures. Compliance will be audited in accordance with relevant OTN audit policy. The Manager, Privacy and Risk (or designate) will be responsible for conducting such audits every two years and ensuring compliance with the policies and its procedures. Issues of non-compliance will be dealt with on an individual basis by the appropriate authority within OTN.

OTN employees and those with whom OTN has a contract to provide goods and services must ensure that this policy and procedures are applied in conjunction with the privacy complaint policy and procedures and determine whether the application of the privacy complaint policy and procedures is warranted.

OTN employees and those with whom OTN has a contract to provide goods and services must ensure that this policy and procedures are applied in conjunction with the policy and procedures for privacy breach management and determine whether the application of the privacy breach management policy and procedures is appropriate.

OTN employees and those with whom OTN has a contract to provide goods and services must also notify the Director, Privacy/CPO (or designate) at the first reasonable opportunity, in accordance with the policy and procedures for privacy breach management, if they breach or believe there may have been a breach of this policy or its procedures.

6.4 PROCEDURE

OTN will make available on its website, information about its privacy policies, procedures and practices. Also, a printed copy of this information as well as more specific information can be requested by contacting the Manager, Privacy and Risk (or designate).

Information regarding the process for making a privacy inquiry is publicly available on OTN's website at www.otn.ca. This process is also outlined in the OTN privacy policy statement, which is also publicly available on OTN's website. The OTN website must indicate that all inquiries must be made in writing and addressed to OTN's Manager, Privacy and Risk. Contact information for the privacy office must be posted on the website.

Once the inquiry is received, the Manager, Privacy and Risk will enter the details of the inquiry into a log of privacy inquiries and a determination will be made regarding the nature of the inquiry and the appropriate response.

Additionally, where appropriate, the provision of printed information concerning OTN's privacy and information security policies and procedures and information regarding the types of data held at OTN will be provided to the inquirer along with reference to the appropriate information on the OTN website.

The Manager, Privacy and Risk (or designate) will respond to the inquiry in writing, and where appropriate, will direct the inquirer to the Health Information Custodian (HIC) that originally collected the personal health information.

7 LIMITING COLLECTION AND USE OF PERSONAL HEALTH INFORMATION

7.1 PURPOSE

To ensure that OTN limits the collection and use of personal health information (PHI) in accordance with the requirements of the Personal Health Information Protection Act, 2004 for Health Information Custodians and their agents.

7.2 POLICY

OTN, minimizes any collection of PHI. Collections are on behalf of Health Information Custodians, particularly when arranging Telehealth sessions. OTN hosts PHI as a result of scheduling Telehealth appointments at the direction of Health Information Custodians (HIC's) and as such acts as an agent for HIC's who input PHI when using the telemedicine network.

As a Health Information Network Provider, OTN only collects personal health information if the Personal Health Information Protection Act, 2004, and its regulations permit the collection.

OTN will collect information by fair and lawful means and will not collect personal health information indiscriminately.

OTN limits the collection of personal health information to what is necessary for its purposes.

OTN does not collect personal health information if other information will serve the purpose.

7.3 RESPONSIBILITY

Director, Privacy/CPO (or designate)

7.4 PROCEDURE

On an annual basis, the Director, Privacy/CPO (or designate) reviews the data elements that are collected to ensure that no more personal health information is being hosted/used or collected on behalf of health information custodians than is reasonably necessary.

7.5 DOCUMENT RETENTION

The Director, Privacy/CPO (or designate) is responsible for securely maintaining a list of approved data elements to be hosted/used or collected as an agent of the health information custodians.

7.6 RELATED DOCUMENTS

List any training/educational/guideline materials for staff.

8 RETENTION, TRANSFER AND DESTRUCTION OF CONFIDENTIAL INFORMATION

8.1 PURPOSE

The purpose of this policy and related procedures is to outline the requirements for retention, transfer and disposal of confidential information received or created by the Ontario Telemedicine Network

(OTN) in accordance with all applicable:

- legal statutes, including the Personal Health Information Protection Act 2004 (PHIPA) and its regulation;
- orders issued by the Information and Privacy Commissioner of Ontario under PHIPA and its regulation, including Orders HO-001, HO-004, HO-006 and HO-007;
- guidelines, fact sheets and best practices issued by the Information and Privacy Commissioner of Ontario pursuant to PHIPA and its regulation, including Fact Sheet 10: Secure Destruction of Personal Information;
- professional regulations;
- accepted research practices; and
- OTN policies, including OTN's privacy policies.

8.2 SCOPE

This policy applies to all OTN individuals who have paper and/or electronic confidential information in their custody or control.

8.3 POLICY

OTN is committed to respecting individual privacy and to safeguarding and ensuring the security of confidential information. To fulfill this commitment, OTN has in place privacy practices and procedures that adhere to the provisions of all applicable laws and guidelines.

8.4 RESPONSIBILITY

Manager, Privacy and Risk (or designate) in coordination with Corporate Security Officer.

8.4.1 General Retention Guidelines

Personal health information (PHI) must be de-identified, where possible, to protect patient privacy. Records containing PHI receive the highest level of protection in accordance with relevant policies and legislation including OTN's general Privacy Policy and PHIPA. Records of PHI may be retained for only as long as necessary to fulfill the purposes for which the PHI is used.

As an agent of a HIC under PHIPA, OTN retains PHI on behalf of health information custodians (HIC's) and follows their data retention policies for grandfathered data as of April 1, 2014. However going forward, to minimize privacy risks OTN does not guarantee future access to PHI hosted on OTN servers beyond 30 days of initial hosting. OTN uses a retention schedule to ensure PHI is retained in accord with legal data retention requirements.

OTN's policy and schedules for the retention, transfer and disposal of records containing personal information, personal health information and de-identified health information, together with legal and professional prudence, must be used to guide decisions to retain records.

Confidential information used for research purposes must not be retained for a period longer than that set out in the written research plan approved by a research ethics board.

All groups at OTN are responsible for ensuring that all electronic and paper records containing confidential information in their work area(s) are retained in a secure manner, in accordance with this policy.

8.4.2 General Transfer Guidelines

Transmission of electronic records containing confidential information via mobile devices, removable media or portable devices from OTN premises must be in accordance with related OTN security policies.

Transmission of paper records containing confidential information must be securely stored and in the custody and control of the individual at all times in accordance with this policy.

Where a third party service provider is contracted by OTN to retain records containing confidential information, a third party agreement must be entered into, in accordance with OTN's policy on third party agreements.

8.4.3 General Disposal Guidelines

Electronic and paper records containing confidential information must be securely disposed. At OTN, secure disposal of paper records of PHI occurs only through the use of third party providers (as described below). The required documentation for the secure disposal of records of PHI by third party providers is as follows:

- the manner for securely transferring, retrieving and/or disposing the records;
- the conditions pursuant to which the records will be transferred, retrieved and/or disposed;
- the agent(s) responsible for ensuring the secure transfer, retrieval and/or disposal of the records;
- documentation of the date, time and mode of transfer of the records;
- maintenance of a detailed inventory of transferred and retrieved records;
- provision of written confirmation to OTN as to receipt of confidential records;
- provision of certificates of destruction immediately following disposal of records confirming the secure disposal of the confidential records, the date, time and method of secure disposal employed, and the name and signature of the agent(s) who performed the secure disposal.

For secure disposal of electronic and/or paper records containing confidential information by third party providers, the above information must be documented in the third party agreement, per OTN's policy on the execution of third party agreements. Certificates of destruction must be provided in accordance with the terms of the third party agreement, and filed by Office Services and the Logistics Coordinator.

Third party service providers engaged by OTN to destroy confidential materials must be bonded and insured with a commitment to confidentiality documented in the third party service provider agreement.

Third party service providers engaged to dispose confidential materials (such as shredding of paper records or electronic media) are to be instructed by OTN as to the appropriate standard to be used, and documented in the third party service provider agreement (e.g., paper should be cross-cut shred to a standard of 3/8" maximum).

Internal disposal of paper records containing confidential information occurs only to the extent outlined in this policy.

Routine destruction of records is prohibited for any documents that are identified as potentially relevant in a known or reasonably anticipated litigation or investigation by a government entity.

8.5 PROCEDURES

8.5.1 Retention of Personal Health Information

OTN treats PHI as having the highest security classification and the highest sensitivity. OTN securely stores electronic records containing PHI and related confidential information accordingly. In addition, various access restrictions are applied according to varying needs and roles. Security and permissions for data residing in electronic repositories must be set by the functional owner of the record in accordance with OTN policies and procedures. A log of these settings will be retained by the CSO.

For paper records OTN securely stores paper records containing confidential information within a locked cabinet or room at all times when unattended. It is the joint responsibility of all OTN staff to ensure confidential records are securely stored pending secure disposal. If an employee notices that confidential materials are not securely stored pending secure disposal, he/she must report non-compliance with this policy immediately to the Director, Privacy/CPO (or designate) or the CSO (or designate), in accordance with OTN's Policy and Procedures for Privacy Breach Management and incident reporting.

8.5.2 Transmission of Confidential Records

Procedure on Sending/Receiving Personal Information, Personal Health Information and De-Identified Health Information and Data Protection - Encryption, Transmission and Storage can be found in Security Policies and Procedures].

8.5.3 Disposal of Confidential Records

In cases where electronic and paper records containing confidential information require compliance with access audit procedures and/or where due diligence requires it, destruction or erasing of these records must be accompanied by a certificate of destruction or the equivalent documentation.

To internally dispose of paper records containing confidential information, paper must be placed into designated confidential waste shredding bins (that are segregated from general recycling bins and are clearly marked and locked) pending their secure disposal. A third party provider, in accordance with this policy, conducts secure disposal of paper records contained within the designated confidential waste shredding bins. OTN staff who telework must use shredders to dispose of confidential paper records.

It is the responsibility of all OTN staff to ensure confidential records are internally disposed in the confidential waste shredding bins. If an employee notices that confidential materials are not securely disposed, he/she must report non-compliance with this policy immediately to the Director, Privacy/CPO (or designate), in accordance with OTN's policy and procedures for privacy breach management.

Failure to provide a certificate of destruction for records containing confidential information immediately following the disposal service, as required by the third party service provider agreement, will be deemed an act of non-compliance with this policy. When a certificate of destruction is not received within the time set out by the service agreement, the OTN contract owner will follow up with the contracted service provider to request that a certificate of destruction be provided.

8.5.4 Retention/Disposal Schedule

OTN maintains a records retention schedule, which is available separately.

("Z:\Departments\Projects and Privacy\Records Management\Retention & Sanitization Schedule V2.0.xlsx")

9 EMPLOYEE EXPECTATIONS OF PRIVACY

While OTN desires to provide a reasonable level of employee privacy, employees should be aware that the information they create on corporate assets remains the property of OTN.

OTN may monitor employee use of OTN assets, including individual log-in sessions logs of telephone, fax, and Internet usage and communications, and may implement appropriate logging and filtering technologies in order to ensure compliance with this policy.

OTN may intercept, monitor, review or disclose any and all messages composed, sent or received on the corporate email system. Employees designated to review messages may include, but are not limited to, an employee's manager and/or representatives from HR and privacy departments.

With the exception of specific incident investigations authorized by OTN human resources, privacy, security, and other senior management, as necessary, OTN will not, without justifiable business requirements (e.g. for telephone call recordings):

- Engage in real-time surveillance of telephone or Internet usage.
- Monitor the content of email, fax or voice mail messages sent or received.
- Disclose any of the logged or otherwise collected information to a third party.

10 PRIVACY TRAINING AND AWARENESS

10.1 PURPOSE

The purpose of this policy is to ensure that a consistent and regular training and awareness program is in place and delivered to relevant agents.

10.2 POLICY

Privacy and security orientation is required for all staff, contractors, students or parties (here in after referred to as agents) who are commencing employment or contractual or other working relationships with OTN that will require access to any OTN stored data, OTN services, OTN premises in any capacity. OTN has a mandatory training requirement for all parties to attend and successfully complete privacy and security training, as well as ongoing training requirements for use of particular OTN services.

All new agents are required to complete initial privacy and security training on the first week of employment/engagement. THERE ARE NO EXCEPTIONS TO THIS POLICY. Upon successful completion of training all AGENTS must sign an OTN confidentiality agreement and annually re-sign this agreement within the first week of each fiscal year. Additionally, third party contractors and vendors sign non-disclosure agreements, as necessary, prior to conducting work for OTN.

10.3 RESPONSIBILITY

Manager, Privacy and Risk, in coordination with Corporate Security Officer and Manager, Training and eLearning,

10.4 PROCEDURES

OTN designates the Manager, Privacy and Risk (or designate) and the Corporate Security Officer (or designate), as jointly responsible for preparing and delivering the privacy and security training. In instances where the training content has changed it must been approved by the V-P Finance and Administration and V-P Innovation and Technology prior to its delivery.

The privacy and security offices will verbally train and orient agents, using an appropriate combination of in-person orientations and online training material and guidelines for particular OTN services, supplemented by information specific to individual roles.

Successful completion of training/orientation will be established through a written test to demonstrate essential privacy and security knowledge. The presenters providing the training will promote an interest in privacy and security knowledge and will communicate that the privacy and security offices are available to all agents for information, clarification, further training, guidance and consultation.

Access to OTN's policy instruments will be provided in both print and electronic formats.

Orientation training in privacy and security is delivered in accordance with the following process:

1) Managers and Human Resources notify the Manager, Privacy and Risk (or designate) concerning new hires commencing employment at OTN.

2) Privacy office staff provides privacy and related security training, using an approved presentation that may be supplemented or customized to the agent's role at OTN.
3) Upon completion of this presentation and test, written materials (*OTN privacy policy, OTN FAQ)* are provided to the trained agent.
4) The OTN confidentiality agreement is signed by the agent.
5) The OTN confidentiality agreement is logged and a copy is retained by the V-P Human Resources (or designate).
6) The privacy and security training and awareness log is updated and reviewed regularly as the dates for the scheduled privacy trainings are booked and documented in the log. No access to OTN information is ever provided until verification by privacy and IS/IT staff is given regarding the completion of the privacy and security orientation. As well, the confidentiality agreement has to been signed and logged by the V-P Human Resources (or designate).
7) The initial privacy and security training and awareness materials are regularly updated and adjusted. At its core, the OTN's the training and awareness package includes out the minimum content for the training in order to ensure some standardization.

It always includes:

- OTN's status under PHIPA and the duties and responsibilities that arise as a result of this status.
- The personal and personal health information (PI/PHI) collected, used and disclosed in the course of OTN provided services.
- The purposes for which PI/PHI is collected, used and disclosed and how this is permitted by PHIPA and its Regulations.
- Limitations placed on access to and use of PI/PHI held by OTN.
- The procedure that must be followed in the event that any agent is requested to disclose PHI;
- An overview of OTN's privacy and security policy instruments and the obligations arising from these.
- The consequences of a breach of the privacy and security policies, SOPs and other procedures, standards, guidelines and practices.
- An explanation of the privacy and security programs, including the key activities of the program and the roles of Director, Privacy/CPO and CSO/Security Lead as well as their respective V-Ps.
- The administrative, technical and physical safeguards implemented by OTN to protect PI/PHI against theft, loss and unauthorized use or disclosure and unauthorized copying, modification or disposal.
- The duties and responsibilities of agents in implementing the administrative, technical and physical safeguards put in place by OTN.
- A discussion of the nature and purpose of the confidentiality agreement that agents must execute and the key provisions of the confidentiality agreement.
- An outline of the OTN Information Breach Policy, which includes the procedures for identifying, reporting and containing a privacy breach. The duties and responsibilities, which are imposed on agents, namely identify, report, contain the breach, to participate in the investigation and assist as requested in remediation of both privacy breaches and information security breaches.

Ongoing privacy and security training will be provided through presentations, updates at monthly staff and team meetings, through electronically distributed privacy updates and print materials, and webcasts. Completion of annual re-training on privacy and security principles using computer-based internal training software is mandatory.

The ongoing privacy and security training also has some standard components to ensure its efficacy. These include:

- Role-based training relating to an agent's day-to-day duties.

- Any new privacy and security policies, standard operating procedures and other procedures, standards, tools, guidelines and practices and significant amendments to existing privacy and security policy instruments.
- Changes made to training modules and/or updates based on recommendations from privacy impact assessment s, the investigation of information security breaches, the conduct of security audits, including threat-risk assessments, security reviews, vulnerability assessments, penetration testing, ethical hacks and reviews of system controls and audit logs.
- Any recommendations with respect to privacy and security training made in privacy impact assessment s, privacy audits and the investigation of privacy breaches and privacy complaints.

Each OTN V-P (or designates) has responsibility for successful completion of security and privacy training by supervised agents. Security and privacy training is mandatory for all individuals who are commencing employment, contractual or other working relationships with OTN that will allow them to work on the premises prior accessing OTN held PI/PHI, OTN's VPN or OTN assets or services.

Failure to attend scheduled training and awareness or retraining sessions will result in the denial of physical access to OTN and immediate revocation of any access privileges.

Confidentiality agreements (non-disclosure agreements in the case of contractors and external service providers) must be signed by all agents engaged with OTN. The OTN privacy training and awareness policy requires all agents to comply with its terms. Compliance is enforced by the V-P Finance and Administration (or designate).

OTN is committed to ensuring a culture of privacy and security at OTN and to ongoing privacy and security awareness outside of its formal privacy and security-training program. The Manager, Privacy and Risk (or designate) will provide timely privacy information to staff and managers on identified outstanding privacy issues, together and mitigation plans. This will be communicated through presentations to affected agents, correspondence, newsletters, and/or postings on OTN's VPN.

A breach of OTN's privacy policy may result in discipline, up to and including termination. As indicated in OTN policy for discipline and termination, compliance will be audited annually in accordance with OTN's audit policy. The Manager, Privacy and Risk (or designate) and CSO/Security Lead will be responsible for conducting the audit. Audit results will be incorporated in the annual privacy report.

The OTN Training and awareness process is as follows:

1) Security and privacy training is provided using a standard approved presentation, which is supplemented and customized to the agent's role at OTN.
2) Upon completion of this presentation, written materials (*OTN Privacy Code*; *OTN Questions and Answers FAQ* and *OTN Privacy and Security Handbook*) are provided to the agent.
3) The agent completes privacy test and if successful score proceeds to the following. Agents are allowed to rewrite the privacy test until a successful score is obtained.
4) The OTN confidentiality agreement or non-disclosure agreement (for contractors) is signed;
5) The OTN confidentiality agreement is logged alphabetically and paper copy is retained in the confidentiality agreement binder by the V-P Human Resources (or designate).
6) In order to ensure compliance with the mandatory re-training requirements, and in accordance with privacy and security orientation policy, OTN maintains a log to track attendance. Privacy office agents are responsible for maintaining this log, which is kept in a shared drive folder for tracking attendance.

10.5 Related Documents

Location of Related Training Documents

10.6 Privacy and Security Training Attendance Logs

In order to ensure compliance with the mandatory training requirements, and in accordance with OTN's privacy and security Training and Awareness Policy, OTN maintains a log to track attendance at both the initial training and the various processes and instruments for ongoing privacy and security training.

The log is the responsibility of the Manager, Privacy and Risk (or designate).

Details regarding the documentation that must be completed, provided and/or executed to verify attendance include:

- Name of agent
- Title of agent
- Supervisor of the agent
- OTN privacy staff who conducted the privacy and security training
- Dates for the following are also logged for each agent.
- Successful score of privacy test upon completion of training.
- Checked attendance of required training and awareness and retraining modules.
- Confidentiality agreement Status.
- Access/Suspension status to OTN held PI/PHI, premises, VPN, OTN services.

11 LIMITING AGENT ACCESS TO AND USE OF PERSONAL HEALTH INFORMATION

11.1 PURPOSE

To ensure the OTN limits access to and use of personal health information by OTN agents as defined below.

11.2 POLICY

An agent is defined as an OTN employee or consultant, contractor or seconded employee to OTN who is authorized to provide services to or on behalf of OTN.

Access to personal health information by OTN agents is role-based and determined by the "need to know" principle. OTN agents are prohibited from accessing or using personal health information except as necessary for his or her employment or contractual responsibilities.

OTN agents are required to access and use the minimum amount of identifiable information reasonably necessary for carrying out their responsibilities.

OTN agents are prohibited from accessing and using personal health information if de-identified or aggregate information will serve the identified purpose

OTN prohibits agents from using de-identified and/or aggregate information either alone or with other information to identify an individual.

11.3 RESPONSIBILITY

Manager, Privacy & Risk

11.4 PROCEDURE

All agents, including employees, consultants, contractors and seconded employees must apply to the Manager, Privacy and Risk for approval to access and use personal health information by completing the agent Data Access Form, which includes:

- The purpose for which access is required.
- The data holdings to which access is required.
- The level of access required.
- The timeframe for access and use.

There are 4 levels of access

- Authority to read.
- Authority to use.
- Authority to disclose.
- Authority to delete.

The application must be signed by the immediate supervisor of the agent and forwarded to the Manager Risk & Privacy along with a copy of the job specifications or contract.

The Manager Privacy & Risk considers the following criteria when reviewing the application for approval:

- The agent routinely requires access to and use of personal health information on an ongoing basis or for a specified period for his employment or contractual responsibilities
- The identified purpose is permitted by the Personal Health Information Protection Act, 2004 and its regulation and cannot be accomplished without personal health information.
- De-identified and/or aggregate information will not serve the identified purpose

If the Manager Risk & Privacy denies access, the Manager Risk & Privacy notifies the agent and his/her supervisor in writing with an explanation of the reasons.

Where the Manager Privacy & Risk approves an application, the Privacy Officer forwards to the agent's supervisor and the System Administrator:

- Name of the agent
- Recommendation for access and use
- Level and type of access and use
- Timeframe that applies to the authorization (if less than one year).

The OTN System Administrator records the information in a log of agents granted approval to access/use/disclose personal health information.

All approved accesses and uses of personal health information are subject to an automatic expiry after one year or sooner based on request.

The Manager Privacy & Risk ensures that all agents sign confidentiality agreement before being given access to personal health information.

11.4.1 Notification and Termination of Access and Use

The supervisor of agents granted approval to access and use personal health information must notify the Manager Privacy & Risk and System Administrator in writing as soon as a decision is taken to terminate or to make any changes in role that would impact the level and type of access and used required by the agent.

The written notification sets out:

- Name of the agent
- Date at which access and use is to be terminated and the reasons for the termination;
- Role no longer requires access
- Employment or contract terminated
- Extended leave of absence
- Any other reason
- The date at which access and use is to change

The OTN System Administrator terminates agent access on the date specified and updates a log of agents granted approval to access/use/disclose personal health information (see section 11.5).

11.4.2 Document Retention

The Manager Privacy & Risk (or designate) is responsible for securely maintaining all files relating to agent access and use of personal health information including:

- agent data access forms and related job specifications/contracts
- Letters of denial of access, where applicable
- Notices of termination/change from OTN supervisors
- Signed confidentiality agreements

The System Administrator securely maintains the log of agents granted approval to access, use, or disclose personal health information.

11.5 Log of Agent Authority to Access/Use/Disclose PHI

This log should record the following information, at a minimum:

- Name of agent
- Level and type of access/use/disclosure
- Any conditions imposed
- Timeframe that applies to the authorization (if less than one year)

11.6 Related Documents

Records Management Policy

12 EXECUTING AGREEMENTS WITH THIRD PARTY SERVICE PROVIDERS

OTN has a third party agreement template. The following section forms the basis of that template and also is the reference when updating the third party agreement template and be used as guidance for specific agreements with HICs

12.1 PURPOSE

To ensure that OTN executes agreements with third party service providers and health information custodians (HICs) based on the expectations set out by the Information and Privacy Commissioner with respect to the protection of personal health information.

12.2 POLICY

A written agreement (Template agreement for All Third Party Service Providers) must be entered into with third party service providers prior to permitting access to and use of personal health information including:

- Those that are contracted to retain, use, transfer or dispose of records of personal health information.
- Those that are contracted to provide services to use electronic means to collect, use, modify, disclose, retain or dispose of personal health information (electronic service providers).

12.3 RESPONSIBILITY

Manager, Privacy and Risk

12.4 PROCEDURE

12.4.1 Agreement Initiation

OTN management initiates agreements with third-party service providers based on OTN procurement policies.

1) OTN management forwards to the Manager, Privacy and Risk, a written request for a third party service agreement. The written request must include:
   a) A description of the task to be performed by the third party.
   b) A copy of the request for proposal or statement of work.
   c) A copy of the successful proposal.
   d) Type and level of personal health information to which the third party will be given access.
   e) Why the function cannot be performed with de-identified and/or aggregate data
   f) Whether personal health information will be removed from the OTN server

2) The Manager, Privacy and Risk creates an agreement, based on the template agreement for all third party service providers and forwards it to V-P Finance and Administration (or designate) for approval.
3) CEO (or designate) executes the third party service provider agreement, provides the third party with one signed agreement and returns one signed agreement to the Manager, Privacy and Risk (or designate).
4) The Manager, Privacy and Risk (or designate) updates a log of agreements with third party service providers. Where information is removed and destruction of the information is required, the Manager, Privacy and Risk (or designate) flags the disposal date for follow-up
5) The Manager, Privacy and Risk (or designate) electronically informs the Director, Privacy and V-P Finance and Administration (or designate) of:
   a) Name of Third Party Service Provider.
   b) Recommendation for access, including type and level of access and use.
   c) Any conditions imposed on access and use (e.g. no access to specified data elements).
   d) Timeframe that applies to the authorization.

12.4.2 Changes to Third Party Service Agreements

OTN management must notify the Manager, Privacy and Risk (or designate) in writing as soon as possible when changes are made to the third party service agreement, including:

- Name of third party provider
- Date at which access is to be terminated, if applicable
- Any changes to the type of access
- Reasons for termination
- The Manager, Privacy and Risk (or designate) informs V-P Finance and Administration (or designate) of changes to access and use of personal health information held in the system and upon V-P sign-off the log of agents granted approval to access/use/disclose personal health information is updated by Manager, Privacy and Risk (or designate).

12.4.3 Disposal/Destruction of Personal Health Information

If the third party service provider agreement specifies retention dates and requirements for secure destruction, the Manager, Privacy and Risk (or designate) ensures that destruction has been completed by the agreed-upon disposal date.

If the third party does not take action within seven days of the date in the third party service agreement, the third party is in breach of the agreement and the Manager, Privacy and Risk (or designate) may take all measures authorized in the agreement. The Manager, Privacy and Risk (or designate) may notify the Information and Privacy Commissioner that the Third Party is in breach and where appropriate lodge a complaint.

12.4.4 Document Retention

The Manager, Privacy and Risk (or designate) is responsible for retaining:

- Request letter from OTN management.
- Third party service provider agreement.
- Log of agreements with third party service providers.

12.4.5 Template for Third Party Service agreement

Available on demand.

13 PRIVACY IMPACT ASSESSMENTS

13.1 PURPOSE

The purpose of this policy is to provide a set of business rules that align with OTN's responsibilities with respect to the protection of Personal Information (PI) as well as Section 6 of Ontario Regulation 329/04 of the 'Personal Health Information Protection Act, 2004 ("PHIPA"). PHIPA requires that OTN, in its capacity as a "health information network provider" ("HINP"), performs an assessment of the services it provides with respect to threats, vulnerabilities and risks to the security and integrity of PHI and reports on how the services may affect the privacy of the individuals who are the subject of the information managed by that service.

According to the Regulation, OTN acts as a HINP when it provides services to two or more health information custodians ("HICs") where the services are provided primarily to custodians to enable the custodians to use electronic means to disclose personal health information to one another, whether or not the person is an agent of any of the custodians. [O. Reg. 329/04, s. 6 (2)]

The Regulation also requires that OTN report a summary of its findings to all applicable HICs.

13.2 SCOPE

All OTN employees, students and consultants must comply with the applicable sections of this policy as a condition of continued employment or engagement.

13.3 POLICY

A privacy impact assessment is a detailed assessment undertaken to identify the actual or potential effects that a proposed project will have on the privacy of those whose personal information is included in the proposed project. A privacy impact assessment also identifies ways in which privacy risks may be mitigated.

OTN must conduct formal privacy impact assessments when acting in its capacity as a HINP to health information custodians, as required by the Personal Health Information Protection Act, 2004. OTN must complete a privacy impact assessment in relation to all new OTN service offerings to health information custodians, or other entities, where those service offerings involve personal health information. Further, OTN must comply with all privacy impact assessment requirements identified in its project funding agreements with Canada Health Infoway.

In all instances, OTN must determine the scope and necessity of conducting privacy impact assessments by first conducting a "privacy threshold assessment" whenever OTN is contemplating a new or modified activity which involves the handling of personal information or personal health information by OTN or through OTN service offerings. A privacy threshold assessment is a preliminary, standardized analysis used to determine whether or not an initiative will require a full privacy impact assessment, an update (or 'delta') to an existing privacy impact assessment, or another level of privacy assurance services, such as an abridged privacy review or consulting services.

OTN undertakes privacy impact assessments or abridged privacy reviews:

- On existing programs, processes and systems when there are significant changes or a significant impact to the way personal information or personal health information is handled either by OTN or through one its service offerings. This requirement extends to OTN's management of personal information related to internal operations, such as human resources and financial information.
- In the design of new programs, processes and systems involving personal health information.
- Any other program, processes and/or system change with privacy implications.

OTN updates privacy impact assessments in the following circumstances:

- During the design and implementation stage.
- Where there is significant change to purposes, data collection, uses or disclosures.
- Where there is significant change to functionality of the service technology.
- Change in vendor/technology partner.
- Every three years, at a minimum.

Privacy impact assessments are not required where existing programs, processes and systems are changed or implemented, if no personal health information or personal information is involved.

The summary results of these assessments will be provided to internal and/or external stakeholders as appropriate, and identified privacy risks will be tracked and monitored for completion by the privacy program using its privacy impact assessment risk register. Summaries of the results of OTN privacy impact assessments may be made available to the public via the OTN website.

All high and medium risks must be mitigated to an agreed upon risk tolerance level (generally this would be a low risk rating) by the project team and PSLT/Champion and/or Sponsor prior to launching or going live with any initiative, program or service. Any exception to this rule must be reviewed/approved by a PSLT/Champion or Sponsor in consultation with the Manager Risk & Privacy.

13.4 RESPONSIBILITY

Manager, Privacy and Risk

13.5 PROCEDURE

OTN management will provide the Director, Privacy/CPO (or designate) with a written description of proposed new programs and/or changes to existing information systems, technologies or programs involving personal health information at the design stage.

The Director, Privacy/CPO (or designate) evaluates the need for a privacy impact assessment. In the case of new programs or changes to existing information systems or technologies involving personal health information, the Manager, Privacy and Risk (or designate) conducts a privacy impact assessment at the design stage to ensure that privacy protections are designed into the new system.

For new programs, the Director, Privacy/CPO (or designate) determines the need and scope of a second privacy impact assessment to be undertaken once the program is implemented to ensure that all recommendations have been implemented.

For changes to existing information systems or technologies, the Manager, Privacy and Risk (or designate) conducts a review upon completion to ensure all recommendations contained in the privacy impact assessment have been implemented.

Where the privacy impact assessment is being outsourced, the Manager, Privacy and Risk (or designate) completes a request for proposal process, executes the contract, monitors the process and receives the completed report and recommendations.
Where the privacy impact assessment is conducted in-house as determined by the Manager, Privacy and Risk (or designate) leads the process.

The Manager, Privacy and Risk (or designate) is responsible for conducting or managing the conduct of privacy impact assessments.

The Manager, Privacy and Risk (or designate) defines the scope and requirements of the privacy impact assessment based on the Privacy Impact Assessment Guidelines for the Personal Health Information Protection Act published by the Information and Privacy Commissioner of Ontario[3] and ensures that the content of the privacy impact assessment includes:

- Information system, technology or program under assessment
- Nature and type of personal health information collected, used or disclosed.
- Sources of the personal health information.
- Purpose of the collection use or disclosure.
- Reason that personal health information is required for the purposes identified.
- The flows of personal health information.
- Statutory authority for each collection, use and disclosure of personal health information.
- Limitations imposed on the collection, use or disclosure of the personal health information.
- Whether or not the personal health information is or will be linked to other information
- Retention period for the personal health information.
- Secure manner in which the records of personal health information will be retained, transferred and disposed of.
- Functionality for logging access, use, modification and disclosure of the personal health information and the functionality for auditing logs for unauthorized use or disclosure.
- Administrative, technical and physical safeguards implemented or proposed to be implemented to protect the personal health information.
- Risks to the privacy of individuals whose personal health information are or will be part of the information system, or technology and an assessment of risks.
- Recommendations to address and eliminate or reduce the privacy risks identified.
- Any threat risk assessments (TRAs) that have been completed
- Any reference documentation.
- The identity of members of the team and contributors.

The Manager, Privacy and Risk submits the completed privacy impact assessment and recommendations to the Privacy and Security Lateral Committee for review and the risks to OTN and action plan with time-frames and required resources to the OTN Senior Leadership Team.

[3] http://www.ipc.on.ca/images/Resources/up-phipa_pia_e.pdf

With the approval of the OTN senior leadership team, the Director, Privacy/CPO coordinates implementation of the recommendations arising from the privacy impact assessment:

- Developing work plans to address risks as identified in the privacy impact assessments and communicating the work plan to the project team
- Assigning action items in consultation with the project team to the appropriate project team member or stakeholder in the organization
- Providing advice, recommendations and support to business areas with regard to managing privacy risks or enhancing privacy in relation to initiatives that are subject to privacy assessment processes
- Tracking and monitoring privacy risk mitigation strategies and reporting on the status of privacy risks as required.

The Manager, Privacy and Risk (or designate) develops and maintains a log of privacy impact assessments.

The Manager, Privacy and Risk (or designate):
Ensures project teams or operational teams provide summaries of privacy impact assessments to relevant health information custodians or OTN service users.

- Communicates privacy impact assessment findings, risks and mitigation recommendations to project teams, internal and external stakeholders.
- Where appropriate drafts summaries of all relevant privacy impact assessments for posting on the OTN websites.
- Tracking and monitoring, through regular reviews, completed privacy impact assessments to ensure their currency.
- Ensures appropriate policy, communication and training are in place to support compliance with this policy and related procedures.

The Manager, Privacy and Risk is responsible for ensuring:

- Privacy impact assessments are planned, budgeted, conducted as necessary and final reports are approved, distributed and published as required by PHIPA and this policy.
- Identified privacy risks are communicated, monitored and managed in accordance with OTN risk management practices.
- OTN maintains appropriate policies, procedures, training and resources to comply with the requirements for privacy risk assessment set out in PHIPA, as well as the requirements set in this policy.
- Appropriate internal and external privacy resources are retained to meet OTN's identified PIA requirements in a timely and effective manner.
- Appropriate communication with and engagement level of OTN's Privacy & Security Lateral Committee and Senior Leadership Team as required to conduct and act on the results of the privacy impact assessment process.
- V-P Finance and Administration approves risk-mitigation action plans prior to submission to and approval by Senior Leadership Team.

13.6 Document Retention

The Manager, Privacy and Risk (or designate) has responsibility for the secure retention of:

- All privacy impact assessments and related documents.
- Log of privacy impact assessment s.
- Timetable for regular privacy impact assessments of existing holdings.

13.6.1 Log of Privacy Impact Assessments

Log contents should include:

- Information system/technology description
- Date PIA completed or expected to be completed
- agent(s) responsible
- PIA recommendations
- Agent responsible for addressing each recommendation
- Date recommendations to be implemented
- Manner in which each recommendation is to be addressed
- Date recommendations implemented

14 PRIVACY COMPLAINTS

14.1 PURPOSE

The Ontario Telemedicine Network (OTN) is committed to addressing promptly any concerns or complaints relating to the management and protection of its data holdings, to OTN's privacy policies, procedures and practices, or to OTN's compliance with the Personal Health Information Protection Act , 2004 (PHIPA) and its regulation.

14.2 POLICY

Any member of the public may challenge OTN's compliance with privacy policies and procedures for the management and protection of personal information including PHI or OTN's compliance with PHIPA and its regulation.

OTN will ensure there is a mechanism for informing the general public about how to initiate a privacy complaint. OTN will ensure there is an internal process in place for receiving and responding to privacy complaints.

OTN will ensure that the general public is aware of their right to forward a privacy complaint to the Office of the Information and Privacy Commissioner of Ontario and how to do so.

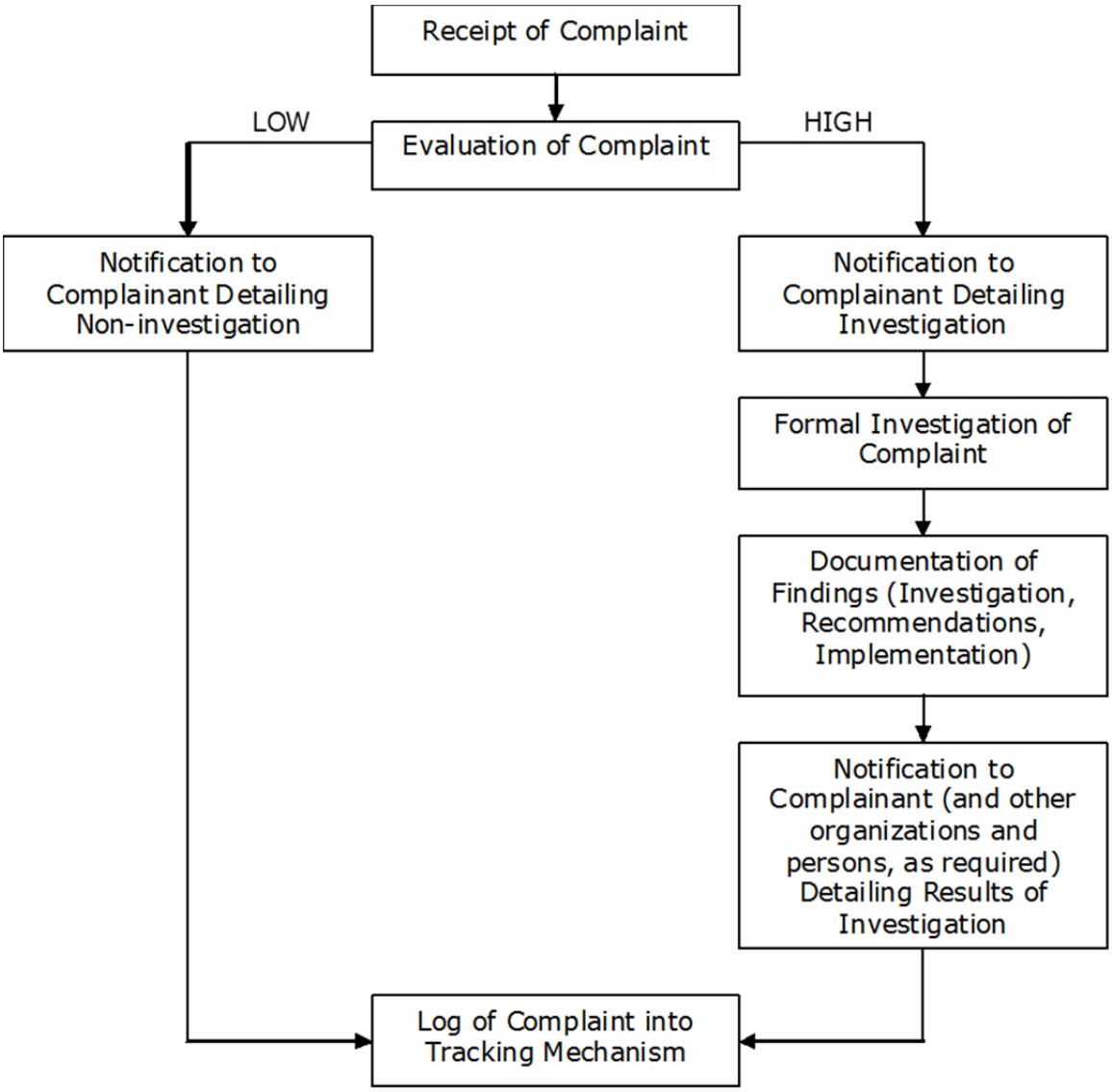
OTN will acknowledge privacy complaints in a timely manner and generally within two business days of the submission of the complaint, provided that the complaint is accompanied by accurate contact information of the complainant.

OTN will formally respond to the complaint within 30 days of the complaint, provided that the complaint is accompanied by accurate contact information of the complainant.

14.3 PROCEDURE

14.3.1 Privacy Complaint Management Process

The figure below identifies the privacy complaint management process employed at OTN.



14.3.2 Receipt of Complaint

Information regarding the process for making a privacy complaint is publicly available on OTN's website at: **http://otn.ca/sites/default/files/18.75.pp_.v2_-_privacy_complaint_policy_and_procedure.pdf**

OTN's website indicates that all complaints must be made in writing and addressed to OTN's Privacy Office. Contact information for privacy must be posted on the website. The Manager, Privacy and Risk designates privacy staff to monitor all incoming complaints and notify the Manager, Privacy and Risk.

OTN's website will also indicate that complaints regarding OTN's compliance with PHIPA and its regulation can be directed to the Information and Privacy Commissioner of Ontario (IPC). The contact information for the IPC is posted on OTN's website.

All complaints made in writing and addressed to the Privacy Office and will be received by OTN and referred to the Manager, Privacy and Risk or designate within two business days of receipt. Upon receipt of the complaint, the Privacy staff designated this responsibility will ensure that the following information has been requested from the individual making the privacy complaint:

- The reason for making the complaint;
- A description of the complaint; and
- The name and contact information of the individual making the complaint.

14.3.3 Evaluation of Complaint

Upon receipt of the complaint, the privacy staff designate will proceed to do the following:

- Enter information into complaint form
- Assess the nature of the complaint and identify and assemble the appropriate OTN staff;
- Determine whether or not the complaint will be investigated (determination within 15 business days), based on the classification of the complaint into one of the following categories:
- All complaints, where PHI has been compromised are considered a high risk.
- Enter the details of the complaint into a log of privacy complaints.

OTN staff will be selected based on the nature of the complaint as identified by the Manager, Privacy and Risk. The Manager, Privacy and Risk, in consultation with the selected staff will review and evaluate all complaints and will investigate those complaints that are deemed to be justified (complaints classified as HIGH).

If a complaint is found to be justified, OTN will take appropriate measures including, if necessary, changes to its policies and procedures. Complaints that are considered to be justified will require a formal investigation. See section 14.3.5 for responding to a complainant where an investigation will be conducted.

If a complaint is found to be minor, the Manager, Privacy & Risk will attempt to achieve an informal resolution without a formal investigation. See section 14.3.4 for responding to a complainant where an investigation will not be conducted.

Within thirty (30) days of the receipt of the complaint, the privacy staff designate will send a written response to the complainant.

14.3.4 Notification to Complainant Detailing Non-Investigation

In situations where a complaint will not be investigated, a written response, approved by the Manager, Privacy and Risk will be sent to the complainant including the following information:

- An acknowledgement of receipt of the complaint;
- A summary of the outcome of the complaint review;
- The nature of the response to the complaint itself including notification that an investigation will not be conducted;
- Information regarding how the complainant may make a complaint to the IPC if there are reasonable grounds to believe that OTN has contravened or is about to contravene PHIPA or its regulation; and
- The provision of contact information for the IPC.

Additionally, where appropriate, the provision of printed information concerning OTN privacy and information security policies and procedures and information regarding the types of data held at OTN will be provided to the complainant along with reference to the appropriate information on OTN's website.

14.3.5 Notification to Complainant Detailing Investigation

In situations where a complaint will be investigated (HIGH classification), a written response will be sent to the complainant, signed by the Director, Privacy/CPO or an appropriate V-P including the following information:

- An acknowledgement of receipt of the complaint;
- A summary of the outcome of the complaint review and the nature of the response to the complaint itself including notification that an investigation will be conducted;
- An explanation of the privacy complaint investigation procedure, indicating whether the individual will be contacted for further information concerning the privacy complaint;
- The projected timeframe for completion of the investigation;
- The nature of the documentation that will be provided to the individual following the investigation;
- Information regarding how the complainant may make a complaint to the IPC if there are reasonable grounds to believe that OTN has contravened or is about to contravene PHIPA or its regulation; and
- The provision of contact information for the IPC.

If the complaint is related to data that has been received from a health information custodian (HIC) and which contains information about the complainant, the complainant will be referred to the HIC where the PHI was originally collected.

If the complainant is not satisfied with the response to the complaint, a personal interview between the Manager, Privacy and Risk (or designate) and the complainant (via phone or in person) may be arranged to review the complaint.

Should this process not address the challenge, the PO will inform the individual that he or she has the option of contacting the IPC and will provide the individual with the contact information for the IPC.

14.3.6 Formal Investigation of Complaint

The investigation of the complaint including the nature and scope of the investigation (e.g., document reviews, interviews, audits) and the process that will be followed in investigating the complaint will be determined by the Manager, Privacy and Risk in consultation with the OTN staff selected at the initiation of the investigation. This consultation shall include a discussion of the following items:

- The documentation that must be completed, provided and/or executed in undertaking the investigation
- The agent responsible for completing, providing and executing the documentation
- The agent to whom this documentation must be provided
- The required content of the documentation

The formal investigation will include the following procedures:

- Clarification of the complaint;
- Gathering of information;

- Completion of a draft report prepared by the Manager, Privacy and Risk or designate which will include a summary of the complaint, a discussion of the information obtained during the investigation, detailed conclusions, and recommendations (if any) to the parties; and
- Provision of a final report.

If warranted, the Director, Privacy/CPO will provide a written report of the investigation to OTN's Board of Directors including recommendations for remediation.

14.3.7 Documentation of Findings

The findings of the investigation, including the recommendations arising from the investigation, the process for implementation, and the recommended timelines for implementation will be included in the investigation report. Subsequently, the Director, Privacy/CPO or designate will be responsible for reporting on the implementation of the recommendations via a written update which will be communicated to the CEO within a designated timeframe that will be determined at the conclusion of the investigation. Communication of the implementation of the recommendations will also be provided to the President.

14.3.8 Notifications

The Manager, Privacy and Risk or designate will be responsible for notifying the complainant (and any/all other organizations and/or persons required to be notified as determined during the formal investigation) in writing, of the outcome of the investigation, within 60 days of the outcome, including the following:

- Findings of the investigation;
- Recommended measures (if any) to be taken in response to the privacy complaint;
- The status of implementation of the recommended measures (if any);
- Information regarding how the complainant may make a complaint to the IPC if there are reasonable grounds to believe that OTN has contravened or is about to contravene PHIPA or its regulation; and
- The provision of contact information for the IPC.

14.3.9 Complaint Log and Tracking Mechanism

The Manager, Privacy and Risk or designate will track all privacy-related complaints by:

- Maintaining a log of all complaints, responses and any remedial action including any relevant documentation;
- Monitoring the implementation of the recommendations arising from the investigation of complaints within the identified timelines; and
- Providing the CEO with a summary of the log on a twice annual basis.

14.4 RESPONSIBILITY

Manager, Privacy and Risk (or designate) and Corporate Security Officer (or designate).

15 PRIVACY REQUEST TO ACCESS OR CORRECT PHI IN OTN CONTROL

15.1 PURPOSE

The Ontario Telemedicine Network (OTN) is committed to addressing promptly any concerns or requests relating to the management and protection of its data holdings, in compliance with the Personal Health Information Protection Act, 2004 (PHIPA) and its regulation.

15.2 POLICY

Any member of the public may request access to their PHI or to correct their PHI
OTN will ensure there is a mechanism for informing the general public about how to initiate an access or correction request. OTN will ensure there is an internal process in place for receiving and responding requests.

OTN will acknowledge requests in a timely manner and generally within 2 business days of the submission that is accompanied by accurate contact information of the requestor.
OTN will formally respond within 30 days of the complaint provided that the request is accompanied by accurate contact information of the complainant.

15.3 RESPONSIBILITY

Manager, Privacy and Risk (or designate), and with the individual who is delegated with the responsibility for the management of the information security program, namely the Corporate Security Officer (CSO).

15.4 PROCEDURE

OTN has forms for requesters, which they are asked to use:

- Access PHI Request: http://otn.ca/sites/default/files/access_phi_request.pdf
- Request for Correction to PHI: http://otn.ca/sites/default/files/request_for_correction_to_phi.pdf

16 PRIVACY AUDITS AND MONITORING REVIEWS

16.1 PURPOSE

The Ontario Telemedicine Network (OTN) is committed to protecting the privacy of the personal information in its custody and control and to demonstrating this commitment to information providers, and to the public.

As part of that commitment, OTN has created the policy and procedures for privacy audits and monitoring reviews, to determine when they will be conducted by OTN and how OTN will respond to the recommendations arising from them.

The purpose of conducting an audit is to assess compliance with the relevant privacy policies, procedures and practices. The purpose of undertaking monitoring reviews is to provide snapshots of up to date information on the day-to-day privacy practices of OTN.

16.2 POLICY

16.2.1 Summary

OTN considers all PHI in its custody to be highly sensitive and implements appropriate safeguards to protect the privacy of individuals whose PHI is received and to maintain the confidentiality of that information. Steps are taken to protect PHI against theft, loss and unauthorized use or disclosure, and to protect records of PHI against unauthorized copying, modification or disposal. Steps also are taken to assess compliance with OTN privacy policies, procedures and monitor day-to-day practices.

16.2.2 Purpose of Privacy Audits

Privacy audits are conducted for the purpose of assessing internal compliance with OTN's privacy policies, procedures and practices that are relevant to the collection, access, use, disclosure, retention and destruction of PHI and external compliance with third party service agreements. The privacy audit will serve as a tool to identify and to address potential privacy issues, to identify non-compliance and to highlight best practices.

The privacy audit will consist of the following elements:

- In person interviews
- A review of documentation (including legislation and regulation for changes under the Personal Health Information Protection Act, 2004 (PHIPA), internal operational policies, procedures and guidelines)
- A review of third party service agreements governing access to and use of PHI that have been entered into third party service providers to monitor compliance with the applicable policies and procedures, including a review of all relevant third party service provider's practices and procedures for reviewing and processing PHI to ensure compliance with the agreement terms
- A report documenting the privacy audit conduct and findings (including recommendations, if any)

The privacy audit demonstrates a commitment to protect all data in the custody and control of OTN and to maintain the public trust in its operations and endeavors.

Monitoring reviews ensure that designated privacy staff periodically check on day-to-day privacy related activities and provide up to date snapshots to the Manager, Privacy and Risk, to detail progress against annual privacy priorities.

16.2.3 Scope of the Privacy Audit

The scope of the privacy audit will be based on the following process:

- Identification of changes in legislation, and regulation for changes under PHIPA;
- Orders, guidelines, fact sheets and best practices issued by the Information and Privacy Commissioner of Ontario;
- Technological advances;
- Recommendations arising from privacy and security audits and privacy impact assessments; investigations into privacy complaints, and privacy and security breaches;
- Review of existing third party service agreements;
- Identification and review of internal documentation (policies, procedures and guidelines) affected by identified changes in legislation and regulation for changes under PHIPA;
- Identification and review of internal documentation affected by changes in operational practices and procedures or affected by new programs/practices;
- Identification and selection of high or low risk operational areas [NTD: reference OTN Corporate Risk Management Policy] governed by internal documentation (policies, procedures and guidelines).

16.2.4 Scope of the Monitoring Review

The scope of the Monitoring Review will be based on the following elements:

- Report to others: Establish a clear purpose and demand for undertaking monitoring, review and evaluation activities. Information produced from this process must be targeted for specific audiences and be incorporated into the governance of OTN in order to enhance transparency and accountability. Activities that occur isolated from decision-making or commence after implementation is complete are of limited value to initiative participants. Monitoring reviews are optimally conducted during the implementation of a program and based on criteria set out in the planning stages of a program.
- Involve stakeholders: Engages all relevant stakeholders for monitoring, review and evaluation activities to be successful. Clearly communicating the benefits of activities and providing the necessary support creates opportunity for willing participation and ownership. An open process that allows stakeholders access to information increases credibility.
- Monitor progress: Delivers timely and relevant information that allows you to track progress towards outcomes and make adjustments to implementation arrangements as necessary. Tracks progress in a deliberate and systematic manner at regular intervals during implementation. Implementation planning must define the data to be collected and the method used for monitoring. Obtaining advice from experts in data collection during the planning process will contribute to a robust and credible methodology. Monitoring will inform other components of implementation such as risk management.
- Review regularly: Incorporates reviews as part of privacy program planning process to assess progress of implementation at critical milestones or in response to specific issues. Reviews are a ‘snapshot’ in the life of an initiative and tend to focus on operational issues, effectiveness of

governance and project management structures, and may also include policy outcomes. Findings and recommendations from reviews should be used to improve implementation.

- Evaluate the outcomes: Identify the extent to which intended and unintended policy outcomes are achieved and how they have affected stakeholders. Planning for evaluation should identify and map baseline information as well as ensure that ongoing access to consistent data sources will be available through monitoring over the life of the initiative. Data can be quantitative (hard or numerical data) or qualitative (soft or categorical). The evaluation will focus on asking good questions to assess the data collected. Credibility of an evaluation is enhanced through sound evidence, professional and ethical standards, and the degree of independence of the evaluator. Effective evaluation is the result of a planning process over the life of the initiative.

16.2.5 Persons Responsible for the Privacy Audits and monitoring reviews

The Director, Privacy/CPO (or designate) will assume primary responsibility for the privacy audit and monitoring reviews

16.2.6 Frequency of the Privacy Audits and Monitoring reviews

At a minimum, the privacy audits will be conducted every two (2) years, or more frequently as required. The frequency of the privacy audit will occur as per defined, pre-scheduled audits as well as ad hoc audits required for cause, or at the request of the Executive Team or any other body that has indicated that an audit is required and that has the authority to request an audit.

Monitoring reviews will be conducted as part of the privacy program cycle and identified in the privacy annual report for the next fiscal year.

The development of the schedule for the privacy audit is the responsibility of the Director, Privacy/CPO and will be developed as per the biennial requirements for the privacy audit. Ad hoc and/or for cause audits will be appended to the schedule at the discretion of the Director, Privacy/CPO.

16.2.7 Log of Privacy Audits and monitoring reviews

Records of all privacy audits and recommendations arising from the audits will be captured in a log of privacy audits that is maintained by the CPO.

Monitoring Reviews will be submitted in the privacy annual report.

16.3 RESPONSIBILITY

Director, Privacy/CPO (or designate)

16.4 PROCEDURE

16.4.1 Conduct of the Privacy Audit and Monitoring Review

Each OTN staff member impacted by a privacy audit or monitoring review will be notified in advance of the start date. This notification will include a schedule for the audit's or monitoring review's conduct including dates and times, the scope of the exercise and the documents and day-to-day procedures to be reviewed (including internal operational policies, procedures and guidelines). The Manager, Privacy and Risk (or designate) will meet with the applicable staff to review all relevant documents and to conduct interviews with the staff to ensure compliance with, and implementation of, the relevant privacy policies, procedures and practices.

In accordance with third party service provider agreements, the Manager, Privacy and Risk (or designate) will provide at least two business days' notice, prior to the assessment and review of a third party service provider's practices and procedures specific to PHI. As per the terms of the third party service agreement, the third party will provide the Manager, Privacy and Risk (or designate) with reasonable access to the policies, procedures and protocols used for purposes of providing the services and any other documents that may be relevant.

The Manager, Privacy and Risk (or designate) will be responsible for completing the audit using a privacy audit report template, documenting the conduct of the privacy audit, including all outcomes.
For monitoring reviews, the Manager, Privacy and Risk (or designate) will be responsible for completing the review using a monitoring review report template, documenting the scope and results of the monitoring review exercise.

The Manager, Privacy and Risk (or designate) will provide a completed copy of the respective privacy audit/monitoring review report templates to the director or leader of the relevant program or platform and to the OTN executive committee through inclusion of a summary in the annual privacy report.

16.4.2 Addressing Recommendations from an Audit or Review

Outcomes of the privacy audit, including all recommendations, will be addressed by Director, Privacy/CPO (or designate) and applicable OTN staff and progress/status will be summarized in the annual privacy report.

Recommendations resulting from the privacy audit will be classified in one of two ways:

- Corrective action request (CAR): a corrective action request is a detailed recommendation which requires timely implementation in order to correct a nonconformance identified through the audit process;
- Preventive action request (PAR): a preventive action request is a detailed recommendation which requires implementation in order to prevent and/or avoid a possible nonconformance identified through the audit process.

Classification of recommendations resulting from the privacy audit will be the responsibility of the PO in consultation with applicable OTN staff where required.

The PO and applicable OTN staff will be responsible for assigning accountability to specific OTN personnel to address the recommendations (CARs and PARs) and for establishing timelines to address the recommendations. The PO will drive rectification of CARs and PARS in a timely manner. Timelines will be based on the schedule and assessment of the recommendations (i.e., ranking of risks).

Outcomes of monitoring reviews, including all recommendations, will be addressed by the Director, Privacy/CPO (or designate) and applicable OTN staff, and progress/status will be summarized in the Annual Privacy Report.

Recommendations resulting from a privacy monitoring review will:
- Identify intended and unintended policy outcomes and how they have affected stakeholders.
- Identify and map baseline information as well as ensure that ongoing access to consistent data sources will be available through monitoring over the life of the target of the monitoring review.

16.4.3 Conclusion of an Audit or Review

At the conclusion of the privacy audit or monitoring review (i.e., when all recommendations have been identified and assigned) the Director, Privacy/CPO (or designate) will provide a report, summarized in the Annual Privacy Report which will include follow up information resulting from the recommendations and the status of their implementation.

16.4.4 Communication of Findings from an Audit or Review

The Director, Privacy/CPO (or designate) will ensure that a report of relevant findings and recommendations from each privacy audit or monitoring review is provided to the OTN Board of Directors.

Relevant information relating to the privacy audit and monitoring review findings (including recommendations) also will be incorporated into the materials for education and training as appropriate.

The outcome of the privacy audit and monitoring review will help keep all stakeholders and staff informed/notified about the access, use, collection and disclosure of PHI including the IPCO, the Ministry of Health and Long Term Care, OTN and the public.

16.4.5 Retention of Privacy Audit Documentation

The Manager, Privacy and Risk (or designate) will retain copies of the reports, which will be made available to the OTN Board of Directors. Relevant leaders of the area being audited will also retain a copy.

The reports will be retained permanently.

All real or suspected privacy and security breaches discovered as a result of the privacy audit or monitoring review will be reported at the first reasonable opportunity to the Director, Privacy/CPO (or designate) or Corporate Security Officer in accordance with OTN's privacy breach management policy.

17 PRIVACY BREACH MANAGEMENT

17.1 PURPOSE

This privacy incident and breach management policy provides guidance to OTN employees, students, consultants and other individuals to take appropriate steps in the event of a privacy incident or breach. This includes particular roles and responsibilities, notification protocols to affected individuals, health information custodians and the Ontario Information and Privacy Commissioner, as appropriate.

In the event of a privacy incident or breach involving PHI and PI occurring in a shared information service or OTN's Telemedicine environment, this policy and procedures sets out the points of responsibility within OTN to respond quickly and effectively by following best practices to monitor, report, contain, notify, investigate, and remediate an incident.

17.2 SCOPE

Although not all incidents result in a privacy breach, all investigations including those related to near misses and non-breach incidents will follow the same process. All employees, students, consultants and other individuals providing services to OTN must comply with the applicable sections of this policy as a condition of continued employment or engagement.

17.3 POLICY

17.3.1 Duty to Report Privacy Incident

Any employee, student, consultant or other individual providing services to OTN who becomes aware of a privacy-related incident has the duty to report that incident as soon as practically possible to the OTN's Privacy Team. The privacy team has the duty to lead the investigation process and, where appropriate, work with other organizations as part of the investigation, follow-up, mediation and response. At the discretion of OTN's Chief Privacy Officer and CEO this may include reporting the incident to affected individuals and the office of the Information and Privacy Commissioner of Ontario.

Upon discovery of an actual or potential privacy incident, OTN shall act immediately to contain the incident to prevent further damage (see section 17.6.3 on containment).

Depending on the scope and severity of the privacy breach, the OTN Director, Privacy/CPO or his or her delegate may escalate the incident details to the OTN senior leadership team in accordance with its escalation process.

All privacy breach documentation is considered a "living" document until the investigation of the incident or breach is satisfactorily concluded and signed off by the OTN Director, Privacy/CPO.

A privacy incident occurs when anyone who has cause to work for or with OTN in its Telemedicine environment:

- Has contravened or is about to contravene a provision of PHIPA or its Regulations;

- Collects, uses or discloses PHI in a shared information service and/or telemedicine environment for purposes other than those described in their roles & responsibilities, agreements and/or policies
- Believes or has reason to believe that PHI or PI has been lost, stolen, or has been used, disclosed, copied or modified in an unauthorized manner;
- Provides access to PHI or PI in a shared information service and/or telemedicine environment to an individual who is not otherwise permitted to access the data;
- Accesses PHI or PI in a shared information service and/or telemedicine environment without authority to do
- Contravenes a requirement set out in OTN's confidentiality agreement with which the user has agreed to comply.

17.3.2 Notification

Where there is a privacy breach in accordance with PHIPA and/or other legislation, OTN will notify all applicable health information custodians (HICs) and/or other applicable stakeholders as required at the first reasonable opportunity.

17.4 RESPONSIBILITY

Director, Privacy/CPO (or designate) and Corporate Security Officer

17.5 ROLES AND RESPONSIBILITIES

All employees, students, consultants and other individuals must report actual and potential incidents and breaches immediately to the Manager, Privacy and Risk or the Corporate Security Officer. Employees, students, consultants and other individuals must contain the incident or breach If capable of doing so, in full cooperation with the Manager, Privacy and Risk and the Corporate Security Officer or their designates.

Under PHIPA, OTN functions as an "agent," and as a "health information network provider" ("HINP"). Therefore it is required to notify any all applicable HICs at the first reasonable opportunity if OTN accesses, uses, discloses or disposes of PHI in a manner inconsistent with its obligations under PHIPA. Notification is also required if OTN becomes aware of any unauthorized access to PHI or PI to allow for hospitals and other applicable stakeholders to comply to their obligations under PHIPA and the Freedom of Information and Protection of Privacy Act (FIPPA).

As such OTN's Manager, Privacy and Risk and Corporate Security Officer or their designates will, in consultation and collaboration with all applicable HICs and other applicable stakeholders, launch and lead privacy breach investigation and incident management processes when it becomes aware of an actual or potential privacy breach.

HICs and other applicable stakeholders are made aware of how to recognize privacy incidents and breaches in a telemedicine environment and their responsibility to notify OTN. Training and communication tools provide the knowledge and awareness necessary to recognize and act on potential incidents and breaches.

17.6 PROCEDURES

17.6.1 Monitoring for Incidents

OTN, healthcare organizations and other stakeholders must monitor their activities to ensure PH and PI in a shared information service and/or telemedicine environment is collected, used, and disclosed within their roles and responsibilities, the terms and conditions of their agreements with OTN, and the requirements of PHIPA and other applicable legislation.

Monitoring activities may include but are not limited to:

- Reviewing information repository audit log reports for unusual or unauthorized activities;
- Reviewing the list of authorized individual with access to share information services and/or telemedicine environment to ensure the list is up to date (e.g., individual roles and responsibilities have not changed);
- Reviewing reports that detail changes to consent directives;
- Reviewing consent overrides (with and without consent) to confirm appropriateness of the action; and
- Receiving, investigating and reporting on privacy incidents and/or complaints made by HICs, clients, the public, and other stakeholders.

17.6.2 Reporting Incidents

All those who work for or with OTN are responsible for immediately reporting privacy incidents or suspected privacy incidents to their Privacy contact person or the Manager, Privacy & Risk and copied to OTN at privacy@otn.ca.

Depending upon the circumstances surrounding the privacy incident, the privacy team may report the incident to:

- HICs, privacy officers and/or members of an affected healthcare organization's organization where their involvement is needed to appropriately address the incident.
- Internal OTN stakeholders including the senior management team in accordance with its escalation process
- Law enforcement, if theft or another crime is suspected (e.g., identity theft);
- Vendors or suppliers that may need to assist in incident containment and resolution and prevention of future incidents;
- Professional or regulatory bodies responsible for disciplining individuals involved in the incident and/or that require notification; or
- The Information and Privacy Commissioner when OTN determines that notification of the IPC is appropriate or required, the IPC's assistance is required to resolve the incident, or the incident may otherwise come to the attention of the IPC.

The privacy incident and the results of the investigation should inform future privacy and security training within the initiative and result in changes to existing policies and procedures as required.

17.6.3 Containing Incidents and Preliminary Assessment

The OTN privacy team must take immediate steps to determine the scope of the incident and contain it. Containment includes, but is not limited to, preventing additional records of PHI or PI from being affected and ensuring that affected records are not further compromised. Measures to do so include the following, to be implemented as necessary in the circumstances:

- Halting unauthorized practices
- Recovering affected records
- Shutting down breached systems
- Revoking network access or changing access codes
- Strengthening physical or electronic security, including temporarily disabling some or all user access to the shared information service or Telemedicine environment)
- Designating qualified lead personnel for preliminary assessment and containment (further investigation may be required)
- Retrieving or ensuring secure destruction of hard or electronic copies of the information that was inappropriately used or disclosed
- Disconnecting a site from a videoconference in progress
- Temporarily not archiving a webcast
- Determining need for a team to further assess problem(s) in detail
- Determining initial communications and escalate internally as appropriate
- Determining if the incident involves theft or criminal activity and, if so, notifying police
- Taking care not to compromise further investigation by compromising or destroying evidence, such as log files, affected information, physical evidence and incident records.

Containment should occur as soon as reasonably possible and should take into consideration the actual or potential severity level of the incident (i.e. critical, high, medium or low). Containment is considered complete when PHI or PI that is the subject of the privacy incident and/or other PHI or PI is no longer at risk of inappropriate collection, use, disclosure or access.

17.6.4 Evaluation of Associated Risks

Once the privacy breach is contained the privacy team will conduct an investigation with the involvement of other parties as necessary to identify and analyze the events that led to the privacy breach or incident, evaluate what was done to contain it and recommend remedial action so future breaches or incidents do not occur.

OTN's privacy team is responsible for investigating the situation at the first reasonable opportunity and to gather the following information:

- The date and time the incident occurred
- Incident type and category (no breach, breach, near miss or non-issue)
- Incident category (videoconference connected in error, etc.)
- A general description of the incident
- The immediate steps that will or have been taken to contain and remedy the incident. (See steps under sections 17.6.3 and 17.6.6.)

The following items need to be considered in assessing the associated risks:

- Personal Health Information involved;
  - Data elements
  - Sensitivity
  - Context

  - Level of encryption/accessibility
  - Potential for fraudulent use
- Causes and Extent of Incident/Breach
  - Determine cause of incident/breach.
  - Determine risk of further exposure of PHI/PI.
  - Determine extent of the unauthorized access to or collection, use or disclosure of personal information, including the number and nature of likely recipients and the risk of further access, use or disclosure.
  - Determine if information lost or stolen and if stolen, was information target of theft or not.
  - Determine status of information recovery.
  - Describe steps taken to mitigate harm.
  - Determine if systemic or isolated problem.
  - Determine number of individuals affected by incident/breach.
  - Determine who is affected: staff, contractors, public, HICs, other organizations.
- Foreseeable Harm
- In assessing the possibility of foreseeable harm from the breach, the privacy team considers the reasonable expectations of the individuals.
- Determine who the recipient of the information is. Is there any relationship between the unauthorized recipients and the data subject? For example, was the disclosure to an unknown party or to a party suspected of being involved in criminal activity where there is a potential risk of misuse? Or was the recipient a trusted, known entity or person that would reasonably be expected to return the information without disclosing or using it?
- What harm to the individuals could result from the breach? Examples include:
  - security risk (e.g., physical safety)
  - identity theft
  - financial loss
  - loss of business or employment opportunities
  - humiliation, damage to reputation or relationships
- What harm to the organization could result from the breach? Examples include:
  - loss of trust in OTN
  - loss of assets
  - financial exposure
  - legal proceedings (i.e., class action suits)
- What harm could come to the public as a result of notification of the breach? Harm that could result includes:
  - risk to public health
  - risk to public safety

The Privacy Team will document the results of the internal investigation. Breach documentation should include:

- The background and scope of the investigation
- How the assessment was conducted
- Cause of the breach
- Inventory of the systems and programs affected
- The reported impact of the privacy breach on those individuals whose privacy was compromised
- Legislative implications
- Determination of the effectiveness of existing security and privacy policies, procedures, and practices
- Findings including a chronology of events
- Recommendations for remedial action

A log of all incidents or breaches, real or suspected, is maintained by the privacy team. High level investigation indicators are documented, tracked and reported in the privacy team's scorecard and shared with the Privacy and Security Lateral Team, the Senior Leadership Team and the Board.

17.6.5 Notifying Individuals of Incidents

Where there is a privacy breach in accordance with PHIPA and/or other applicable legislation, OTN will notify all applicable health information custodians (HICs) and other appropriate stakeholders at the first reasonable opportunity.

It is not OTN's role to notify the individual(s) to whom the breached PHI or PI belongs, but it is OTN's responsibility to notify the HIC or other stakeholder of the breach. The HIC or other stakeholder will then notify, as required, the individual(s) whose PHI or PI was disclosed.

The purpose of providing notice of a privacy breach to the subject individual(s) is to provide information about the incident, the nature of potential or actual risks or harm, what mitigating actions are being taken and appropriate future action for individuals to take to protect their information.

Healthcare organizations are required to notify individuals (patients/clients) whose PHI was stolen, lost, or accessed by unauthorized persons, as well as collected, used or disclosed in a manner or for a purpose not permitted by PHIPA.

Notification to affected individuals should be made by the impacted organization where only one HIC is involved or through mutual consensus of the impacted organizations where multiple organizations are involved. Where possible, the HIC with the closest relationship to the client should provide the notice if it is impacted by the incident.

Notification must include:

- The date of the incident
- A general description of what happened
- A description of the PHI or PI inappropriately accessed, collected, used or disclosed
- The steps taken to control or reduce the harm and steps planned to prevent further incidents
- The steps affected individuals can take to protect themselves, if applicable (e.g., how to contact the MOHLTC for OHIP monitoring)
- The contact information of an individual who can provide further information or assistance and
- How to make a complaint to the IPC

17.6.6 Remediation

The privacy team will establish a remediation plan to address the potential cause(s) of the incident and minimize the likelihood of identical or similar incidents from reoccurring. A remediation plan should include the following, as appropriate to the specific incident:

- A detailed description of the remediation activity (e.g., a review of relevant information management systems, any amendments or reinforcements to existing policies and/or practices, development and implementation of new security or privacy measures, testing and evaluating remedial plans and training of staff)
- Designation of individual(s) responsible for implementing remediation
- Description of any need for amendment or reinforcement of existing policies, procedures, or practices for managing and safeguarding PHI or PI

- Recommendations related to the development or implementation of new security or privacy measures, if required
- A review of employee training to reduce potential or future breaches, and recommendations to strengthen it as required
- Recommendations for remedial action to the appropriate internal and external stakeholders
- Escalation of more wide scale or complex remedial actions to OTN's Enterprise Risk Management committee

17.6.7 Prevention of Future Breaches

Once the immediate steps are taken to mitigate the risks associated with the breach, OTN will investigate the cause of the breach and consider whether to develop a prevention plan. The level of effort should reflect the significance of the breach and whether it was a systemic breach or an isolated instance. This plan may include the following:

- a security audit of both physical and technical security;
- a review of policies and procedures and any changes to reflect the lessons learned from the investigation and regularly after that (e.g., security policies, record retention and collection policies, etc.);
- a review of employee training practices; and
- a review of service delivery partners (e.g., HICs, contractors, service providers).

The resulting plan may include a requirement for an audit at the end of the process to ensure that the prevention plan has been fully implemented.

17.7 REFERENCES

The Personal Health Information Protection Act, 2004 and Ontario Regulation 329/04:
http://www.ipc.on.ca/english/Home-Page/

Freedom of Information and Protection of Privacy Act:
http://www.e-laws.gov.on.ca/html/statutes/english/elaws_statutes_90f31_e.htm

Privacy Investigation Automated Process Map 2012

For more information the IPC has published a number of documents which are available on the website: www.ipc.on.ca

- What to do when faced with a Privacy Breach: Guidelines for the Health Sector
- Breach Notification Assessment Tool
- Frequently Asked Questions: Personal Health Information Protection Act
- A Guide to the Personal Health Information Protection Act

17.8 RELATED DOCUMENTS

Subject	Number
Summary of Privacy Investigation form	
Privacy Investigation log	
Privacy Breach Checklist (appended per section 23.3)	

18 TERMINATION OF EMPLOYMENT/CONTRACTUAL RELATIONSHIP

18.1 PURPOSE

This policy and its procedures ensure a documented process that provides continued protection of PI and PHI upon termination or cessation of employment.

As part of OTN's broader termination policy and procedures regarding the following privacy-related components are incorporated.

18.2 POLICY

OTN has a Leaving the Organization Policy and exit procedures, which ensure that affected OTN managers, directors and the CEO are notified of any employee or service provider terminations in instances where these parties had access to personal information or personal health information. This includes all employment and contractual relationships.

It is OTN's policy that all OTN property, including access cards, identification badge, computer equipment, electronic devices and office and filing cabinet keys are returned and logged when returned prior to leaving the premises.

18.3 RESPONSIBILITY

Vice President Human Resources

18.4 PROCEDURES

Termination of employment-resignation & discharge procedure:

- The determination to discharge an employee from employment at OTN must be made in consultation with the Vice President Human Resources or delegate and communicated to the Manager, Privacy and Risk as well as the Corporate Security Office.
- The agent's leader will communicate to staff the departure/termination of identified agent(s) in accord with broader OTN HR procedures.
- OTN ensures that all relevant policies, legislative requirements are adhered to and the discharge is completed in a humane and caring manner.
- Director responsible for Security and his/her staff in the Information Systems Department must be notified in advance to ensure that access to OTN computers, OTN's VPN, email, voice mail and buildings is terminated at the time of discharge.
- The responsible Director/Manager will ensure that all OTN property such as files, documents, identification badge, keys, cell phones, laptop computers, passwords, have been secured prior to the person leaving the premises.
- The Corporate Security Office or designate, at the time of notification of discharge, will cancel all access for the agent to OTN premises, to locations within the premises where records of personal health information are retained and to the information technology operational environment immediately upon termination or cessation of employment, contractual or other relationship;

- The Corporate Security Office or designate will log status of secured items and access controls noted in this policy and report any exceptions to the VP Human Resources.
- The Manager, Privacy and Risk or designate will be responsible for auditing logs and reporting to OTN's CEO on a quarterly basis for access termination and secured and outstanding items as Part of OTN's privacy audit policy and procedures.
- VP Human Resource or delegate will follow-up directly within 2 business days with terminated parties to secure outstanding items and escalate as necessary, including notifying IPC, if willful non-compliance and, with IPC guidance, seek lawful means to retrieve unsecured items/information as deemed appropriate.
- Consequences for failure to comply with termination protocol is detailed in OTN employment/contracting agreements and will be treated as a privacy and security breach according to OTN's Breach Policy and Procedures.
- The Director, Privacy/CPO (or designate) and the Corporate Security Office will notify the VP Human Resources at the first reasonable opportunity, if an agent may have created or discovered a breach of this policy or its procedures.

19 EXECUTION OF CONFIDENTIALITY AGREEMENTS BY AGENTS

19.1 PURPOSE

The purpose of this policy is to ensure that a framework exists for having all agents sign required confidentiality agreements in a set time frame.

19.2 POLICY

Agents are responsible for safeguarding the confidentiality of corporate, proprietary, personal and personal health information (referred to as 'confidential information') whether in verbal, written or electronic form. In order to communicate these obligations clearly, OTN requires agents to undertake a confidentiality agreement prior to accessing this type of information.

OTN's confidentiality agreements (as provided in section 23.1) must be signed by OTN employees, students, consultants, or other individuals providing services to OTN within a week of starting work. The confidentiality agreements must be re-signed each year within one month of the start of OTN's fiscal year.

Failure to sign the confidentiality agreement will result in denial of physical access to all OTN facilities and OTN-held or managed personal information or personal health information. The Corporate Security Office or designate will be notified of anyone failing to sign their agreement by the Vice President, Human Resources (or designate). Upon receipt of notification the Corporate Security Office or designate will suspend all information access privileges until such time as the confidentiality agreement is signed.

19.3 RESPONSIBILITY

Vice President Human Resources

Each employee is responsible for ensuring they understand the confidentiality policy, procedure and agreement and for obtaining answers to any questions they may have with their immediate supervisor or human resources personnel.

19.4 PROCEDURES

The Leader (or designate) of each OTN department, as part of their job specifications, are accountable and responsible for ensuring that a confidentiality agreement is duly signed in the time-frames noted above for all staff, consultants and other individuals associated with their department. The Leader (or designate) is responsible for notifying the Vice President Human Resources or designate of new staff, consultants, students and other individuals two weeks prior to those individuals being engaged with OTN. Notification will be by correspondence.

The Manager, Privacy and Risk (or designate), in coordination with the Manager, Training and e-Learning, will notify by correspondence OTN employees, consultants, students and other individuals of the need for privacy and security training prior to signing the confidentiality agreement. Upon receipt of notification the OTN employees, consultants, students and other individuals to whom this applies must successfully complete the privacy training and orientation established by OTN.

Successful completion will require a score of 80% or higher on a privacy quiz as determined annually by the Manager, Privacy and Risk (or designate) and undertaken at the completion of the training and orientation.

Annual signing of confidentiality agreements require staff to first score 80% or higher on the privacy quiz for that fiscal year.

The Vice President Human Resources or designate will log alphabetically and retain paper copies of signed confidentiality agreements. The Vice President Human Resources or designate will notify by correspondence the responsible director if any individual under that director's auspices does not meet the timelines.

Confidentiality agreements will be subject to annual Privacy Audits by the Manager, Privacy and Risk or designate (see section 16). Any breach of conditions of the confidentiality agreement will be subject to the Policy and Procedures for Privacy Breach Management (see section 17).

20 DISCIPLINE AND CORRECTIVE ACTION INVOLVING AGENTS

20.1 PURPOSE

The purpose of this policy and procedures is to ensure any privacy breach created by an agent is dealt with in a fair and equitable manner that respects the PHIPA and OTN's commitment to protecting the PI/PHI in its custody and control.

20.2 POLICY

OTN's Vice President of Human Resources, will be notified by the Director or Manager of any agent requiring corrective or disciplinary action resulting from non-compliant activities regarding personal and or personal health information.

20.3 RESPONSIBILITY

Vice President, Human Resources

20.4 PROCEDURES

The Vice President of Human Resources or designate, in coordination with the Director, Privacy/CPO (or designate), has responsibility for the investigation of failures to protect personal information and personal health information, and for determining corrective action or discipline for such failures. Such investigations will also address whether any breach of contracts of employment, consulting services, or other services have occurred.

The investigation protocol will involve a review of relevant documents, documentation regarding the non-compliant action or privacy breach, determination of the impact of the breach (e.g., minor internal only, OTN reputational, illegal behavior under PHIPA , or life-threatening) and factors (e.g., unintentional, training related, willful ignorance, malicious intent) that need to be weighed in determining a course of action.

A report will be submitted to the VP, Human Resources outlining the impact, factors and a course of action. The course of action may range from cautionary correspondence, through mandatory training, probation and monitoring for a set period of time, to suspension, termination or prosecution.

Upon finalization and approval of the determined corrective and or disciplinary action by the VP, Human Resources, the director of the non-compliant agent will implement the course of action and include the course of action and report in the agent's HR file. The Manager, Privacy and Risk (or designate) will also keep the course of action and related documentation. An aggregate summary of such investigations and actions will be included in the annual privacy report to the CEO.

The director or manager of any agent requiring corrective or disciplinary action resulting from non-compliant activities regarding personal and or personal health information will notify OTN's Manager, Privacy and Risk (or designate).

The VP Human Resources in coordination with the Director, Privacy/CPO (or designate) are responsible for investigating and determining corrective action/discipline for non-compliant activities regarding personal and or personal health information.

The protocol for the investigation will involve review of relevant documents, documentation regarding the non-compliant action or privacy breach, determination of the impact of the breach (e.g. minor internal only, OTN reputational, illegal behavior under PHIPA, or life-threatening) and factors (e.g. unintentional, training related, willful ignorance, malicious intent) that need to be weighed in determining a course of action.

A report will be submitted to VP Human Resources outlining the impact, factors and a course of action (from cautionary correspondence, through mandatory training, probation and monitoring for a set period of time to suspension or termination and prosecution).

Upon finalization and approval by the VP Human Resources, the Director/Manager of the non-compliant agent will implement the course of action and include the course of action and report in the agent's HR file and will notify the Manager, Privacy and Risk of the actions taken. An aggregate summary of such investigations and actions will be included in the annual privacy report to the CEO.

21 CONSOLIDATED LOG OF PRIVACY ISSUES AND RECOMMENDATIONS

21.1 POLICY

OTN maintains a log of privacy issues and recommendations. The Director, Privacy/CPO, the CSO or designates will monitor and update the log regarding implementation of recommendations. The Privacy Director/CPO will include a summary of the log as part of the annual privacy report.

21.2 RESPONSIBILITY

Director, Privacy/CPO (or designate)

21.3 PROCEDURES

The Manager, Privacy and Risk (or designate) maintains a corporate log of all privacy impact assessment , privacy audit, investigated privacy breaches, privacy complaints and privacy and security breaches, together with their related recommendations and their implementation status. The log also contains recommendations stemming from the Office of the Information and Privacy Commissioner of Ontario.

The log is reviewed by the OTN CEO on an annual basis. The Manager, Privacy and Risk (or designate), in coordination with the Corporate Security Officer, performs log updates and reviews the log on a quarterly basis or at the completion of any privacy event, whichever comes first.

Audits of compliance with implemented recommendations will be led by the Manager, Privacy and Risk (or designate) on an annual basis. Please see the policy and procedures for privacy audits and monitoring reviews in section 14 for more detail.

Failure to adhere to this policy will be treated as a privacy breach and the policy and procedures for privacy breach management apply (see Section 17).

The log should contain the following information, at a minimum:

- Source (PIA, IPC, Audit, etc.)
- Date
- Issue Description
- Recommendation(s)
- Mitigation Measures
- Completion Date(s) for Mitigation Measures
- Staff Responsible

22 CORPORATE PRIVACY RISK REGISTRY

22.1 RESPONSIBILITY

Director, Privacy/CPO (or designate)

22.2 PROCEDURES

OTN maintains a corporate Privacy Risk Registry. The Privacy Risk Registry is summarized in the Annual Privacy Report, using the following Table.

Identified Risk	Assessment of Risk	Risk Level/Rank (high, medium, low)	Mitigation Strategy/Date of Implementation	Potential for Recurrence	Post Mitigation Impact if Recurrence	Person of Accountability

The OTN Privacy Risk Registry is updated annually by the Manager, Privacy and Risk (or designate) and included in the annual privacy report submitted to Executive Committee and the CEO for approval. In addition, at the prerogative of the Manager, Privacy and Risk (or designate), background reports can be appended that take an OTN-wide view of privacy and information security risks and addresses the following:

- Linked risks and risk drivers;
- A ranking of the risk; likelihood score/impact score = risk rating;
- Mitigation actions implemented;
- Retained (Net) Risk;
- Any additional mitigation required;
- Risk owners.

23 APPENDICES

23.1 CONFIDENTIALITY AGREEMENT

Authority to access and use confidential information is associated with, and restricted by, the job duties of each person working at OTN. Each OTN employee, contracted worker or other agent is accountable for ensuring that confidential information is strictly limited to information that an individual requires for the performance of his or her job duties. Access to, use and disclosure of this information is limited on a "need-to-know" basis and predicated on having a valid, signed confidentiality agreement. Signed agreements are valid for up to one year, at which point a new agreement must be duly signed.

Note: OTN legal counsel should review and approve the format and contents of the agreement before it is implemented.

23.1.1 Responsibility

Director, Privacy/CPO (or designate) in coordination with Vice President, Human Resources

23.1.2 Confidentiality Agreement Template

23.1.2.1 Preamble

I acknowledge that I have read, understand and have successfully completed the Ontario Telemedicine Network's (OTN's) Training and Orientation of its Privacy and Confidentiality Policies.

Further, I understand that:

- OTN is established and maintained to provide telemedicine services for Ontarians;
- Such telemedicine services depend on access to personal and personal health information (PI/PHI) subject to statutory and other obligations to protect PHI through Ontario's Personal Health Information Protection Act, S.O. 2004, c3.
- Confidential Information for purpose of this agreement includes, OTN's personnel, corporate, proprietary information, any personal and personal health information held by OTN, as well as information about its relationship to its service providers and other third parties is confidential information.
- OTN will only permit access to OTN confidential information for up to one year, upon signature of this agreement.
- OTN requires that I re-sign a confidentiality agreement on an annual basis within one month of the beginning of OTN's fiscal year.

23.1.2.2 Purpose of this agreement

This agreement sets out the terms and conditions governing my access, use and disclosure of Confidential Information as set out in the preamble of this agreement regarding any and all confidential information, personal and personal health information available through OTN.

This agreement is valid for up to one year upon signature and dating.

23.1.2.3 Protection of Confidential Information

I agree to protect confidential information available through OTN by:

- Successfully completing Privacy & Security Testing on an annual basis where required
- Protecting confidential information by:
  - i. Using it for the purpose it was provided, unless prior written permission is obtained from OTN Director, Privacy/CPO (or designate).
  - ii. Disclosing confidential information only to persons who are authorized by OTN to receive such information (i.e., have a valid, signed confidentiality agreement or as permitted under PHIPA), and only to the extent required to conduct OTN services.
  - iii. Protecting and keeping secure computer access codes (for example, passwords).
  - iv. Using physical security protection for access devices (for example, keys and badges).
  - v. Refraining from lending my access codes or devices to anyone, or attempting to use those of others.
  - vi. Accepting legal responsibility for work done under assigned access codes and devices.
  - vii. Not removing, altering, destroying, copying or interfering with confidential and/or personal health information, except with written authorization and in accordance with OTN policies and procedures.
  - viii. Upon Removable, taking all necessary steps to protect confidential information against unauthorized use or disclosure.
  - ix. Securely returning or destroying confidential information, as requested, in accordance with OTN procedures.
  - x. Notifying immediate supervisor and OTN Privacy Manager immediately if in receipt of any legal or other demand to disclose confidential information.
  - xi. Notifying immediate supervisor and OTN Privacy Manager immediately of any failure, or potential failure, to protect confidential information in accordance with this agreement.
  - xii. Co-operating with any investigation or review by Ontario's Information & Privacy Commissioner, the Ministry of Health and Long Term Care, OTN, or lawful investigation under PHIPA.

23.1.2.4 Terms and Termination

I understand and by signature, accept the entirety of this agreement.

Failure to comply with this confidentiality agreement may result in disciplinary action up to and including termination of my employment or affiliation with OTN and may also result in legal action being taken by OTN, member sites, or patients.

My obligations under this confidentiality agreement survive indefinitely past the termination of any relationship with OTN.

This agreement is in addition to and not in substitution of any and all other obligations to OTN.

This agreement shall be governed by and construed in accordance with the laws of Ontario and Canada.

The courts of Ontario shall have non-exclusive jurisdiction with respect to this agreement.

OTN has the right to disclose that I have entered into this agreement.

23.1.2.5 Signature Block

I understand and by signature, accept the entirety of this Confidentiality.

Name (please print)	**Signature**	**Date**
Witness (please print)	**Signature**	**Date**
Supervisor (please print)	**Signature**	**Date**

This agreement is valid up to one year from the date of completion by Supervisor.

23.2 OTN AGENT DATA ACCESS/USE FORM

Name of agent requesting access and/or use:

Position and title at OTN: _____

Name of OTN Supervisor: _____

Request is for:

- ☐ Access only
- ☐ Access and use

Level of access required:

- ☐ Authorization to read
- ☐ Authorization to use
- ☐ Authorization to disclose
- ☐ Authorization to delete

Data for which access is requested: _____

_____

_____

_____

Data for which use is requested: _____

_____

_____

_____

Why is this level of access or use required? _____

_____

_____

_____

Start date of access/use: _____

Termination date of access/use: _____

Signature

Agent

Name (print): _____

Signature: _____

Supervisor

Name (print): _____

Signature: _____

23.3 PRIVACY BREACH CHECKLIST

For more details, please see *Key Steps for Organizations in Responding to Privacy Breaches*.[4]

23.3.1 Incident Description

- What was the date of the incident?
- When was the incident discovered?
- How was it discovered?
- What was the location of the incident?
- What was the cause of the incident?

23.3.2 Step 1: Breach Containment and Preliminary Assessment

- Have you contained the breach (recovery of information, computer system shut down, locks changed)?
- Have you designated an appropriate individual to lead the initial investigation?
- Is there a need to assemble a breach response team? If so, who should be included (e.g., privacy officer, security officer, communications, risk management, legal)?
- Have you determined who needs to be made aware of the incident internally and potentially externally at this preliminary stage?
- Does the breach appear to involve theft or other criminal activity? If yes, have the police been notified?
- Have you made sure that evidence that may be necessary to investigate the breach has not been destroyed?

23.3.3 Step 2: Evaluate the Risks Associated With the Breach

- What personal information was involved?
  - What personal information was involved (name, address, SIN, financial, medical)?
  - What form was it in (e.g., paper records, electronic database)?
  - What physical or technical security measures were in place at the time of the incident (locks, alarm systems, encryption, passwords, etc.)?
- What was the cause and extent of the breach?
  - Is there a risk of ongoing breaches or further exposure of the information?
  - Can the personal information be used for fraudulent or other purposes?
  - Was the information lost or was it stolen? If it was stolen, can it be determined whether the information was the target of the theft or not?
  - Has the personal information been recovered?
  - Is this a systemic problem or an isolated incident?
- How many individuals have been affected by the breach and who are they (e.g., employees, contractors, public, clients, service providers, other organizations)?

[4] https://www.priv.gc.ca/information/guide/2007/gl_070801_02_e.asp

- Is there any foreseeable harm from the breach?
  - What harm to the individuals could result from the breach(e.g., security risk, identity theft, financial loss, loss of business or employment opportunities, physical harm, humiliation, damage to reputation, etc.)?
  - Do you know who has received the information and what is the risk of further access, use or disclosure?
  - What harm to the organization could result from the breach (e.g., loss of trust, loss of assets, financial exposure, legal proceedings, etc.)
  - What harm could come to the public as a result of notification of the breach (e.g., risk to public health or risk to public safety)?

23.3.4 Step 3: Notification

- Should affected individuals be notified?
  - What are the reasonable expectations of the individuals concerned?
  - What is the risk of harm to the individual? Is there a reasonable risk of identity theft or fraud?
  - Is there a risk of physical harm? Is there a risk of humiliation or damage to the individual's reputation?
  - What is the ability of the individual to avoid or mitigate possible harm?
  - What are the legal and contractual obligations of the organization?
  - If you decide that affected individuals do not need to be notified, note your reasons.
- If affected individuals are to be notified, when and, how will they be notified and who will notify them?
  - What form of notification will you use (e.g., by phone, letter, correspondence or in person, website, media, etc.)?
  - Who will notify the affected individuals? Do you need to involve another party?
  - If law enforcement authorities are involved, does notification need to be delayed to ensure that the investigation is not compromised?
- What should be included in the notification?
  - Depending on the circumstances, notifications could include some of the following, but be careful to limit the amount of personal information disclosed in the notification to what is necessary:
  - information about the incident and its timing in general terms;
  - a description of the personal information involved in the breach;
  - a general account of what your organization has done to control or reduce the harm;
  - what your organization will do to assist individuals and steps individuals can take to reduce the risk of harm or further protect themselves;
  - sources of information designed to assist individuals in protecting against identity theft;
  - contact information of a department or individual within your organization who can answer questions or provide further information;
  - whether your organization has notified a privacy commissioner's office;
  - additional contact information to address any privacy concerns to your organization; and
  - contact information for the appropriate privacy commissioner(s).
- Are there others who should be informed about the breach?
  - Should any privacy commissioners' office be informed?
  - Should the police or any other parties be informed? This may include insurers; professional or other regulatory bodies; credit card companies, financial institutions or credit reporting agencies; other internal or external parties such as third party contractors, internal business units not previously advised of the privacy breach, union or other employee bargaining units)

23.3.5 Step 4: Prevention of Future Breaches

- What short or long-term steps do you need to take to correct the situation (e.g., staff training, policy review or development, audit)?

End of Document