ONTARIO TELEMEDICINE NETWORK

Integrated Privacy Policy Framework

Prepared with assistance from

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**
Valorie Tutt	Director, Legal and Regulatory Affairs	July 2019
Pal Gill	Vice-President Finance and Administration	July 2019

Revision History

VERSION NO.	**VERSION DATE**	**SUMMARY OF CHANGE**	**CHANGED BY**
V.1	December 20, 2013	Initial draft	Excela Associates
V.2	February 10, 2014	Revisions, post January 2014 review by privacy team.	Excela Associates
V.3	March 13, 2014	Revisions based on review of Action Register Items	Excela Associates
V.4	June 10, 2015	Updated with approved edits	Henry Bury
V.5	August 3, 2017	Review and update	Sylvie Gaskin / Henry Bury
V.6	February 7th 2018	Review and update	Sylvie Gaskin
V.7	December 11, 2018	Initial Draft of Integrated Privacy Policy Framework	Excela Associates
V.8	January 14, 2019	Review and update	Sylvie Gaskin

V.9	July 16, 2019	Review and update	Valorie Tutt/Michelle MacMillan

Contents

1 PREAMBLE

1.1 GLOSSARY

1.1.1 Definitions

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

TERM	DEFINITION
Agent	An agent is defined under PHIPA in relation to a health information custodian, which means a person/organization that, with the authorization of the custodian, acts for or on behalf of the custodian in respect of personal health information for the purposes of the custodian, and not the agent's own purposes, whether or not the agent has the authority to bind the custodian, whether or not the agent is employed by the custodian and whether or not the agent is being remunerated. In this Integrated Privacy Policy Framework, OTN refers to its employees, contractors, volunteers, students and any other parties who are commencing employment, contractual or other working relationships with OTN as agents.
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, 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	Confidential information is any information given or used in confidence that may be disclosed only to authorized individuals on a need-to-know basis and includes personal health information (PHI), personal information (PI) and information consolidated for regulatory purposes. Confidential information also includes information related to business operations such as employee agreements, financial or business records and contracts.

TERM	DEFINITION
Consumer	A resident of Ontario that logs into and provides personal information (enrolls) for one or more of the Direct to Consumer Services provided through OTN's web site (named otn.ca/patients). A consumer is anyone in the public who can access service from OTN who doesn't have to go through a Physician to access OTN. Example: physician and OHIP number involved = patient. Anything outside that would be a consumer.
Fair Information Principles (FIPs)	The ten privacy principles embodied in the Canadian Standards Association's *Model Privacy Code* of 1996 and in the *Personal Information Protection and Electronic Documents Act* (PIPEDA).
Direct to Consumer Services (DtC services)	The DtC services include: otn.ca/patients, Facebook, Twitter, available to the general population. It is important to distinguish DtC service from OTN patient services; namely services where a patient is registered with or receiving a service from or goes through a physician for a service. A consumer is anyone in the public who can access service from OTN who doesn't have to go through a Physician to access OTN. Example: If a physician and/or OHIP number are required to deliver service, the person is a patient. Otherwise the person is a consumer.
DtC Services Staff	Any and all staff involved in managing the various services available to consumers through www.otn.ca/patients, OTN's Facebook or Twitter accounts.
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;

TERM	DEFINITION
	• 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; 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. • Non-PHI Incident - Situation was reported and investigated but not found to be a privacy breach or a near miss.
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.
otn.ca/patients	An OTN web site to facilitate consumers accessing and using various health services (e.g., Heart Failure Monitoring & Coaching, eVisit Appointments, Mental Health Support, Immunization Management, Problem Gambling Support), named: otn.ca/patients.
Personal Health Information (PHI)	Identifying information about an individual in oral or recorded form, if the information 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 provider of health care to the individual, is a plan of service within the meaning of the *Long-Term Care Act, 1994* for the individual, relates to payment or eligibility for health care in respect of the individual, relates to the donation by the individual of any body part or bodily substance of the individual or is derived from the testing or examination of any such body part or bodily

TERM	DEFINITION
	substance, is the individual's health number or identifies an individual's substitute decision-maker (Personal Health Information Protection Act, 2004, s.4(1)). Identifying information means information that identifies an individual or for which it is reasonably foreseeable in the circumstances that it could be utilized, either alone or with other information, to identify an individual (Personal Health Information Protection Act, 2004, s.4(2)).
Personal Information (PI):	Personal Information means information about an identifiable individual. 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, business email address or telephone number of an employee of an organization.
Personal Information Protection and Electronic Documents Act (PIPEDA)	Federal legislation that sets privacy requirements for organizations covered under the Act and uses the Fair Information Practices to detail those requirements.
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

TERM	DEFINITION
	health information are subject to unauthorized copying modification, or disposal.
Privacy Impact Assessment (PIA)	A formal assessment of privacy risk associated with a given service, project or information system.
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 PI and 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

TERM	DEFINITION
	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.

TERM	DEFINITION
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.

TERM	DEFINITION
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
- *A guide for Business and Organizations: Privacy Tool Kit, Canada's Personal Information Protection and Electronic Documents Act*, published by Canada's Office of the Privacy Commissioner.
- *A Privacy Framework for Mobile Health and Home-Care Systems*, published by David Kotz, Dartmouth College NH, et al.

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 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
Business Continuity Policy	05.08.P
Physical Security Policy	21.06.P
Mobile Computing and Storage Devices Policy	21.15.P
Change Management Policy & Procedure	21.01.PP
Access Control Security Policy	21.26.P
Logging and Monitoring Policy	21.21.P
Threat Risk Management Policy & Procedure	21.07.PP
System and Software Development Lifecycle Policy	21.47.P
OTHER TOPICS COVERED UNDER THE INFORMATION SECURITY POLICY 21.42.P	
Security Program Management, Governance and Oversight	
Information Security Training	
Information and Asset Management	
Business Continuity and Disaster Recovery	

1.3 COMPLIANCE

OTN staff, contractors, 3rd party service providers and volunteers must be compliant with this policy and its procedures. Violations will include all breaches of confidentiality of OTN information, including consumer personal information (PI) collected through otn.ca/patients. 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 (or designate) and/or the Information Security Manager at the first reasonable opportunity, in accordance with Policies and Procedures for Privacy Breach Management and 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 (or designate) and the Information Security Manager (or designate) must notify each other of potential breaches and incidents that come to their attention.

Where it is clearly a privacy breach the first point of notification is the Manager, Privacy. For clear security breaches the Information Security Office is the first point of notification.

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 Manager, Privacy (or designate), 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.
- Voluntarily adhere to privacy best practices as set out in the Fair Information Principles (FIPs) as detailed by Canada's Office of the Privacy Commissioner (OPC) in instances where consumer personal information is held by OTN as part of its Direct to Consumer services offered through www.otn.ca/patients.

The Framework has been developed with two reference points:

- The Information and Privacy Commissioner of Ontario's (IPC) Manual for the Review and Approval of Prescribed Persons and Prescribed Entities[1] for consistency with the privacy standard expressed therein, although OTN is not a prescribed entity under PHIPA.
- The Fair Information Principles as detailed by the OPC.

2.2 POLICY

The Chief Executive Officer of OTN is accountable for ensuring that OTN individuals and any contracted 3rd parties comply with:

- The Personal Health Information Protection Act, 2004 and its regulations.
- The Fair Information Principles as set out by the OPC in their Privacy Toolkit for Businesses and Organizations and included in OTN's Integrated Privacy Policy Framework.
- OTN privacy policies and procedures.

The Chief Executive Officer of OTN has delegated day-to-day management for privacy to the Manager, Privacy.

The Manager has responsibility for the overall function of the privacy program, planning and strategy, as well as supporting the Senior Leadership Team (SLT) in implementing various initiatives and services. The Manager is counted on to identify privacy risks and opportunities for executive's consideration and business decisions. The Manager may delegate some day-to-day responsibility to members of the Privacy team as appropriate. The Manager participates in OTN Leadership Team (OLT) meetings and has management responsibilities for the implementation of OTN privacy policies and procedures, as well as the day-to-day management of privacy activities at OTN.

The Manager, Privacy, has full time dedicated staff members to whom specific obligations may be assigned to address privacy and information management requirements and issues. In carrying out the day-to-day responsibilities of the OTN privacy program, the Manager, Privacy, is supported by the

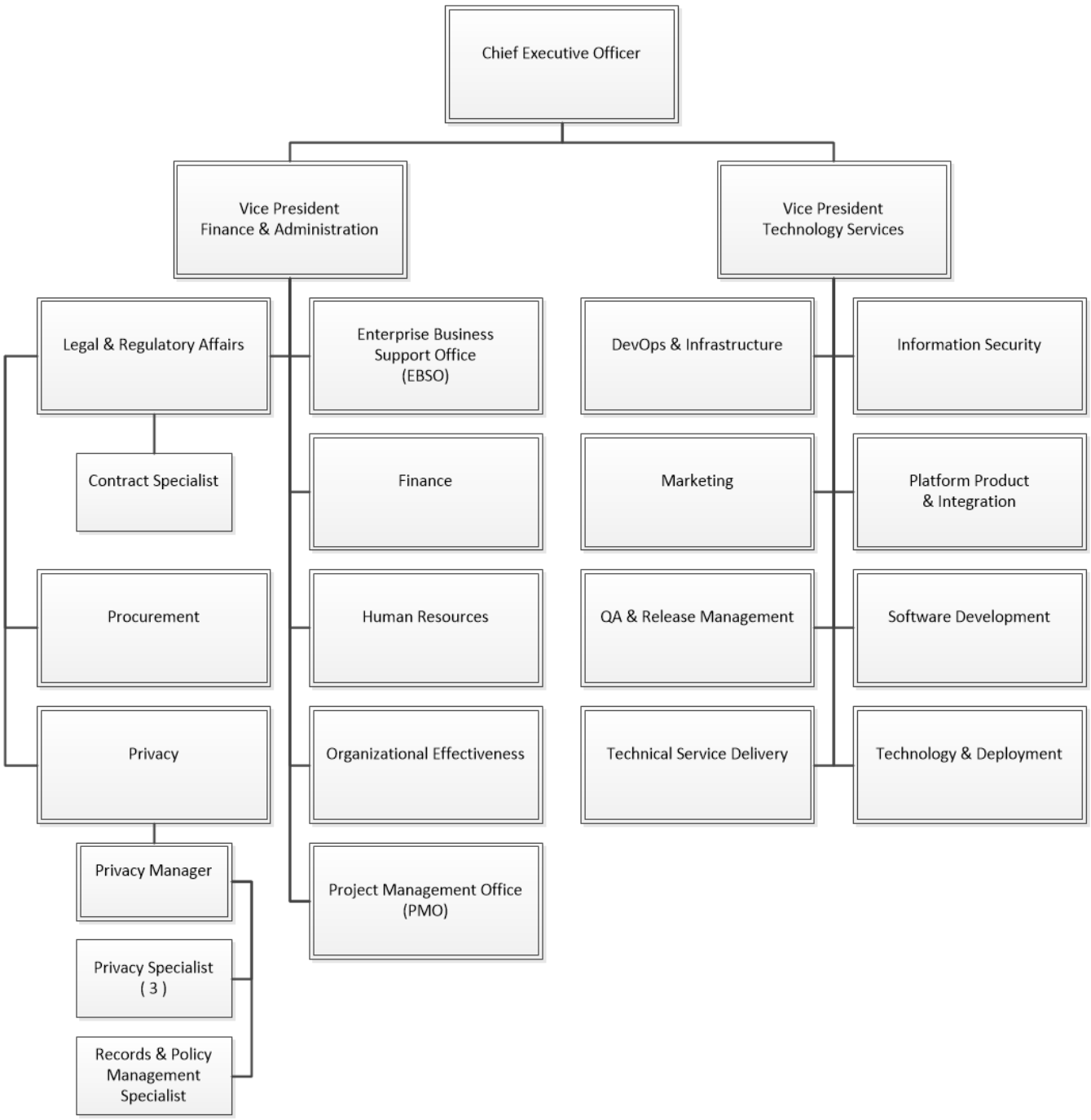
[1] *Manual for the Review and Approval of Prescribed Persons and Prescribed Entities,* Information and Privacy Commissioner of Ontario, 2010, http://www.ipc.on.ca/images/Findings/process.pdf.

Director, Legal and Regulatory Affairs, and the SLT.

The Director, Legal and Regulatory Affairs has administrative responsibility for the Manager, Privacy.

2.3 ACCOUNTABILITY GOVERNANCE STRUCTURE

OTN's governance structure as follows:



2.4 PROCEDURES

The Manager, Privacy (or designate) develops the OTN Annual Report on Privacy Compliance and Strategy for the Privacy and Security Lateral Team. The Manager finalizes the OTN Annual Report on Privacy Compliance and Strategy in discussion with Director, Legal and Regulatory Affairs and with the VP Finance & Administration.

The content of the OTN Annual Report on Privacy Compliance and Strategy includes:

- A description of privacy training provided for staff.
- Review of consumer-facing personal information management, communications, achievements and issues.
- 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.
- Bi-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 timelines, and resource requirements.

The OTN Annual Report on Privacy Compliance and Strategy is reviewed by the Director, Legal and Regulatory Affairs, Vice-President, Finance and Administration, and the Privacy and Security Lateral Team. The OTN Annual Report on Privacy Compliance and Strategy is then forwarded to the Chief Executive Officer of OTN, who provides it to the OTN Planning Priorities Committee of the Board of Directors.

The Manager, Privacy (or designate) works with the OTN Communications team to post the OTN Annual Report on Privacy Compliance and Strategy on the OTN website.

The Manager, Privacy (or designate) ensures that the OTN Accountability Framework, as well as the organization chart, is included in OTN privacy training.

3 JOB ACCOUNTABILITIES FOR DELEGATED PRIVACY AND SECURITY POSITIONS

The Manager, Privacy has responsibility for the overall function of the privacy program, planning and strategy, as well as supporting the SLT in implementing various initiatives and services and externally handles all Chief Privacy Officer inquiries and communications. The Manager is counted on to identify privacy risks and opportunities for executives' consideration and business decisions. The Manager may delegate some day-to-day responsibility to members of the Privacy team as appropriate. The Manager participates in OTN Leadership Team (OLT) meetings and has management responsibilities for the implementation of OTN privacy policies and procedures, as well as the day-to-day management of privacy activities at OTN.

The Manager, Privacy is deemed the main privacy OTN point of contact for legislative purposes.

The following identify the points of accountability for privacy and security. The roles and associated job titles referenced below are current as of the publishing date for this document. Role changes occurring after the publishing date will be incorporated during the next review period.

3.1 VP FINANCE AND ADMINISTRATION

The VP Finance and Administration's job accountabilities have the following components listed as key responsibilities and obligations for privacy and OTN, to be undertaken in compliance with relevant OTN policies and procedures:

- Provides executive oversight and guidance to his/her direct report.
- Provides executive review for any materials, strategies, issues prior to engaging the CEO, Board members or senior executives as identified by the Director, Legal and Regulatory Affairs.
- Reviews and approves privacy initiatives in support of new lines of OTN business.
- Reviews and approves substantial changes to OTN privacy training.

3.2 DIRECTOR, LEGAL AND REGULATORY AFFAIRS

The Director, Legal and Regulatory Affairs job accountabilities has the following components listed as key responsibilities and obligations for privacy and OTN, to be undertaken in compliance with relevant OTN policies and procedures:

- Provides oversight and guidance to his/her direct report.
- Provides review for any materials, strategies, issues prior to engaging the VP Finance and Administration, Senior Executives as identified by the Manager, Privacy.
- Reviews and approves privacy initiatives in support of new lines of OTN business.
- Reviews and approves changes to OTN privacy training before going to the VP Finance and Administration.

3.3 MANAGER, PRIVACY

The Manager 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, standards and guidelines (together, referred to as policy instruments).
- Ensure compliance with privacy policies and procedures.
- Advise management, senior executives and CEO of privacy risks, issues and opportunities.
- Provide to the Director, Legal and Regulatory Affairs and VP Finance and Administration 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.
    - Facilitate adherence to FIPs best practices for OTN-managed PI as a result of its DtC Services.
    - Ensure staff, agents, vendors, consultants, service providers are aware of:
        - PHIPA and its Regulation and their duties, obligations and responsibilities in relation to PHIPA.
        - FIPs, as detailed by the OPC and integrated in this Privacy Policy Framework.
    - Direct, deliver or ensure the delivery of the initial privacy orientation and the ongoing privacy training and fostering a culture of privacy.
    - In co-ordination with Human Resources and legal counsel (as required) establish consistent practices to address willful failure to comply with OTN's privacy policies, FIPs, and PHIPA for OTN's workforce and business partners.
    - 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 of Ontario regarding PHIPA compliance.

Manager, Privacy includes the following in the Manager, Privacy responsibilities. OTN also has identified the Manager, Privacy, reporting to the Director, Legal and Regulatory Affairs, 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, adherence to FIPs where consumer PI is involved, and OTN privacy policy and procedures.
- Develop compliance contingency plans in consultation with departments and project teams when compliance to PHIPA, adherence to FIPs where consumer PI is involved 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 Director, Legal and Regulatory Affairs to review and monitor third party privacy agreements, internal staff confidentiality agreements, information notices, legal practices and requirements under PHIPA and adherence to FIPs where consumer PI is involved.
- Serve as OTN's liaison with the Office of the Information and Privacy Commissioner (IPC) regarding PHIPA compliance and other privacy matters as deemed discussable with the IPC.
- Coordinate findings and mitigation or escalation strategies through the Director, Legal and Regulatory Affairs, and the VP, Finance and Administration.
- In collaboration with the Information Security team, ensure alignment between security and privacy practices and where alignment cannot be reached, escalate to VP Finance and Administration and VP Technology and Services.

3.4 VP Technology and Services

The VP Technology and Services' job accountabilities has the following components listed as key responsibilities and obligations for security and OTN, to be undertaken in compliance with relevant OTN policies and procedures:

- Provides executive oversight and guidance to his/her direct report.
- Provides executive review for any materials, strategies, issues prior to engaging the CEO, Senior Executives as identified by the Director, DevOps and Infrastructure.
- Holds management responsibility for the Director, DevOps and Infrastructure.
- Reviews and approves security initiatives in support of new lines of OTN business.
- Reviews and approves substantial changes to OTN security training.

3.5 Director of DevOps and Infrastructure

The Director of DevOps and Infrastructure at OTN has been delegated the day-to-day responsibility and authority to manage the OTN security program. The Manager of Information Security reports directly to the Director of DevOps and Infrastructure through to the VP Technology and Services. 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:

- Provides oversight and guidance to his/her direct report.
- Provides review for any materials, strategies, issues prior to engaging the VP Technology and Services, Senior Executives as identified by the Manager, Information Security.
- Reviews and approves security initiatives in support of new lines of OTN business.
- Reviews and approves changes to OTN security training before going to the VP Technology and Services.

3.6 MANAGER, INFORMATION SECURITY

OTN also has identified the Manager, Information Security reporting to the Director, DevOps and Infrastructure. The Manager has the following key responsibilities and obligations, to be undertaken in compliance with relevant OTN policies and procedures:

- Develop, implement, review and amend security policies, practices, procedures, standards and guidelines (policy instruments).
- Ensure compliance with the security policy instruments implemented.
- Ensure staff, vendors, consultants and agent service providers are aware of OTN security policy instruments and are appropriately informed of their duties, obligations and responsibilities.
- Oversight on the development, implementation, review and amendment of security policies, practices, procedures, standards and guidelines (together, referred to as policy instruments).
- Ensure compliance with security policies and procedures.
- Advise management, senior executives and VP Technology and Services of security risks, issues and opportunities.
- Provide to the Director, DevOps and Infrastructure and VP Technology and Services the necessary support of the security program and facilitate the following:
    - Ensure that security policy instruments are transparent, accessible and understood.
    - Ensure staff, agents, vendors, consultants, service providers are aware of all relevant security policies and practices.
    - Direct, deliver or ensure the delivery of the initial security orientation and the ongoing security training.
    - Determine needs for system-wide and project-specific Threat Risk Assessments.
    - Oversee the management of security complaints.
    - Oversee the management of security inquiries.
    - Provide direction for managing security breaches or suspected security breaches.
    - Determine needs for security audits and program reviews.
    - Identify trends, both positive and negative, in security management within OTN.
- 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 guide the ongoing review and development of its privacy policies and procedures to support the evolving business.

4.2 POLICY

OTN undertakes a review of its privacy policies and procedures on a biannual 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, initiates a review of privacy policies and procedures:

- Bi-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 the Ontario Office of the Information and Privacy Commissioner (IPC) and/or the Office of the Privacy Commissioner (Canada) issues an Order, Fact Sheet, Guideline and/or best practice applicable to OTN's business or practices.
  - When amendments are made to the Personal Health information Protection Act, 2004 (PHIPA) and its regulation that are relevant to OTN.
  - When changes are required.

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

- Concerns raised by OTN agents, application service providers and health information custodians.
- Recommendations arising from complaints and inquiries.
- Consumer feedback for OTN's Direct to Consumer Services (DtC Services).
- Recommendations arising from privacy audits and investigations into privacy breaches.
- Recommendations arising from privacy impact assessments.
- Orders, guidelines, fact sheets and best practices issued by the IPC and/or the Office of the Privacy Commissioner (Canada).
- Relevant amendments to PHIPA and its regulation.
- Evolving industry standards and best practices.
- Inconsistencies between privacy policies and actual practice.

Recommendations for significant change are forwarded to the OTN Policy Office where they will be directed for review and approval by the policy sponsor as appropriate, in consultation with the VP, Finance and Administration.

When approval has been obtained, the Manager, Privacy (or designate):

- Upon posting, sends a memorandum to all senior management and staff (as required) 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.
- Distributes relevant information on changes to policies or procedures to service providers as required.
- Flags relevant training materials for possible revisions.
- Identifies existing agreements that may require amendments to reflect changes.

The Manager, Privacy (or designate) ensures that the annual review process, development of amendments or changes, and communication of those changes, are completed in accordance with established review and renewal timelines.

5 TRANSPARENCY OF PRIVACY POLICIES AND PROCEDURES

5.1 PURPOSE

To ensure that OTN's privacy policies and procedures are easily understood, open and transparent for consumers of the services available via www.otn.ca/patients, 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 and the personal information held as a result of OTN's Direct to Consumer (DtC) Services.

Contact information for designated staff in OTN's Privacy Office will be published on OTN's websites and made available to members of the public through Telemedicine Coordinators and Primary Contacts at referring and consulting sites. The OTN Privacy Office may also be reached via email at privacy@otn.ca.

OTN's applicable privacy policies are posted on the OTN's websites (www.OTN.ca and www.otn.ca/patients). They are also available to members and/or members of the public on request to OTN's Privacy Office. A printed privacy policy framework is also available upon request.

OTN's descriptions of services and safeguards taken to protect personal and personal health information will be posted on OTN's websites and are also available to members of the public on request to OTN's Privacy Office and via email at privacy@otn.ca.

5.3 PROCEDURE

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

The Manager, Privacy (or designate) ensures that the information on the websites at www.otn.ca and www.otn.ca/patients includes:

- A description of OTN privacy policies.
- Frequently asked questions related to OTN privacy policies and procedures.
- A general description of personal and personal health information retained by OTN.
- Summaries of privacy impact assessments conducted by OTN.
- Name, title, mailing address and contact information of the designated staff at the OTN Privacy Office to whom inquiries, concerns or complaints regarding privacy compliance may be directed.
- The email address for the OTN Privacy Office (privacy@otn.ca).

The Manager, Privacy (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 and personal health information.
- Types of personal and personal health information collected on each OTN website.

- Health information custodians and other sources from whom this information is typically collected.
- The purposes for which personal and personal health information are collected.
- The purposes for which personal and personal health information are 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 at the OTN Privacy Office to whom inquiries, concerns or complaints regarding privacy compliance may be directed.

Instructions for making complaints are posted on OTN's websites and may be obtained through OTN Privacy Office staff or Telemedicine Coordinators/Primary Contacts at OTN Member sites[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 or personal health information contained therein.

Updates to public and stakeholder materials are addressed per OTN's Policy on Ongoing Review of Privacy Policies (section 3 in the OTN Integrated Privacy Policy Framework).

[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 as set out in the Integrated Privacy Policy Framework 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 (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 Manager, Privacy (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 (or designate).

Information regarding the process for making a privacy inquiry is publicly available on OTN's website at www.otn.ca. For consumer-facing services the first point of contact on www.otn.ca/patients is the email contact point: privacy@otn.ca. For non-OTN services on www.otn.ca/patients, email contact points are included in the privacy statements of non-OTN services. These contact points and the inquiry process are also outlined in the OTN privacy policy statement, which is also publicly available on OTN's websites. The OTN websites must indicate that all inquiries must be made in writing and addressed to OTN's Manager, Privacy. Contact information for the privacy office must be posted on the websites.

Once the inquiry is received, the Manager, Privacy (or designate) 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 relevant OTN website.

The Manager, Privacy (or designate) will respond to the inquiry in writing, and where appropriate, will direct the inquirer to the Health Information Custodian (HIC) where the collection of personal health information occurred. For consumer-related privacy inquiries that cannot be resolved by OTN and/or non-OTN services, a resolution process will be identified by the Manager, Privacy.

7 IDENTIFYING PURPOSE(S) FOR COLLECTION

7.1 PURPOSE

To ensure that OTN has set out and/or reviewed specific collection purposes for any of the Direct to Consumer (DtC) services on the team and self-managed virtual care website accessible at otn.ca/patients prior to implementation.

7.2 POLICY

OTN ensures that each DtC service identifies and documents prior to implementation:

- what personal information (PI) will be collected from consumers;
- why each element is needed with a view to narrowly defining the purpose to prevent harm from wrongful collection; and
- how it will be used and/or disclosed by the DtC service.

OTN will ensure that any new purpose will be reviewed prior to implementation of new uses/disclosures of PI.

The purpose statement for collection documentation will stress clarity of purpose in plain language that will be communicated to consumers.

7.3 PROCEDURES

Manager, Privacy, or designate will:

- Ensure that purposes for collection are reviewed and identified as part of the Privacy team's project consultation services.
- Initiate a monthly review of written PI requirements of each DtC service against the stated PI needs stemming from the DtC service's purpose.
- Review annually the notices in the various media (written, Consumer Relation Management (CRM) scripts, website notices) used to communicate to consumers. The review will pay special attention to communications alignment with the characteristics of the consumers (including but not limited to age, language facility, and health concerns) and the purpose each DtC service has for collecting PI elements.
- Initiate monthly review of PI held by OTN for each DtC service.
- Ensure the Data Governance Working Group (DGWG) performs an annual review of the data holdings of a program against the program's stated purpose and data requirements.
- Ensure the purposes of collection for DtC services are aligned with the reasonableness principle, namely that a reasonable person would expect specific collection and support the stated purposes for that collection.

8 MANAGING CONSENT

8.1 PURPOSE

To ensure that consumers of Direct to Consumer (DtC) services understand the nature and purpose of their express consent for the collection, use and/or disclosure of their Personal Information (PI) for the team and/or self-managed virtual care service they wish to use, accessible at otn.ca/patients.

8.2 POLICY

OTN ensures DtC services:

- Provide team and/or self-managed virtual care consumers with easily understood statements of what PI elements are collected and why the service collects that PI.
- Obtain team and/or self-managed virtual care consumer's consent prior to or at time of PI collection and prior to a new use of PI already collected.
- Detail the purpose(s) for collection that is easily understood by all consumers.
- Inform team and/or self-managed virtual care consumers of the benefits and risks involved in providing PI through team and/or self-managed virtual care services.

8.3 PROCEDURES

Manager, Privacy (or designate) will:

- Review consent protocols for each DtC service to ensure informed consumer consent.
- Ensure consumer facing communications explain in plain language how the PI collected will be used and/or disclosed.
- Determine placement of communications for ease of access by team and/or self-managed virtual care consumers.
- Take into consideration supplementing the main consent notice with privacy notifications and explanations within the DtC service that address particular consumer communications challenges (e.g., age, health, mother tongue).
- Ensure that a log or record of proof of informed consent is available upon request.
- Review consumer facing communications that explain implications of consent withdrawal and ensure communications align with the DtC service's stated purpose(s).
- Provide documentation, training and education to both OTN and DtC service staff to ensure both are equipped to answer consumer questions regarding the purpose and use/disclosure of the PI collected.

9 LIMITING COLLECTION OF PERSONAL AND PERSONAL HEALTH INFORMATION

9.1 PURPOSE

To ensure that OTN limits the collection 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.

To ensure OTN limits collection of personal information (PI) through www.otn.ca/patients in accordance with Fair Information Principle (FIP) best practices as set out by the Canadian Standards Association's *Model Privacy Code* of 1996.

9.2 POLICY

OTN minimizes any collection of PI and PHI. PHI collections are on behalf of Health Information Custodians (HICs), particularly when arranging Telehealth sessions. OTN hosts PHI as a result of scheduling Telemedicine appointments at the direction of HICs and, as such, acts as an agent for HICs 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 collects PI directly through www.otn.ca/patients and informs consumers that PI collection is necessary to achieve the stated purposes of each Direct to Consumer (DtC) service.
OTN and the DtC services on www.otn.ca/patients will collect information by fair and lawful means and will not collect personal health information indiscriminately.

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

OTN does not collect personal or personal health information if other information will serve the purpose.
OTN ensures clear communications to consumers of DtC services the reasons for collecting PI.

9.3 RESPONSIBILITY

Manager, Privacy (or designate)

9.4 PROCEDURE

On an annual basis, the Manager, Privacy (or designate):

- Ensures that the DGWG reviews the data elements that are collected to ensure that no more personal or personal health information is being hosted/used or collected than is reasonably necessary on behalf of health information custodians and in relation to the services available via www.otn.ca/patients.
- Ensures OTN employees, staff, contractors, 3rd party service providers, volunteers and www.otn.ca/patients service providers can explain to consumers why the PI collected is necessary for the operation of DtC services, through appropriate documentation, training and education.

On a bi-monthly basis, the Manager, Privacy (or designate):

- Ensures that the DGWG reviews the PI collected with a view to reducing the PI collected and held for DtC services.

9.5 DOCUMENT RETENTION

The Manager, Privacy (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.
- Securely maintaining a list of approved PI data elements held by OTN as a result of consumers' use of www.otn.ca/patients.

10 LIMITING USE AND DISCLOSURE

10.1 PURPOSE

To ensure that OTN limits the 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.

To ensure OTN restricts the use and disclosure of Personal Information (PI) held to the purpose for which the PI was initially collected.

To ensure OTN provides privacy protective advice to consumers.

10.2 POLICY

OTN ensures annual review of the uses and disclosures of PI and PHI against the stated purposes for collection.

OTN ensures documentation and approval by Manager, Privacy (or designate), and informed consumer consent for any new purpose or use of PI subsequent to its collection.

OTN ensures DtC services set out policies with regard to the types of PI that need to be updated based on reasonable circumstances (e.g., address changes).

OTN ensures annual review of advice to consumers to protect their PI and reduce or eliminate unauthorized disclosure from their devices.

10.3 PROCEDURES

Manager, Privacy (or designate):

- Reviews documentation for new uses and purposes prior to implementation.
- Reviews annually the written requirements for PI uses and disclosures for DtC services against each service's purpose statement and data requirements to ensure collection is not expanded beyond the initial service scope or OTN Policy.
- Reviews annually various DtC services for PI data elements that may require periodic updating to ensure accuracy.
- Reviews monthly, consumer notices to ensure adequacy and currency of methods and steps consumers can take to protect their PI from unauthorized access or viewing.

11 ACCURACY

11.1 PURPOSE

To minimize the use of incorrect or out-of-date Personal Information (PI) when providing Direct to Consumer (DtC) services and/or when disclosing PI to third parties within the team and self-managed virtual care services.

11.2 POLICY

OTN requires periodic review of held PI from DtC services to ensure the information is accurate and up to date.

11.3 PROCEDURES

Manager, Privacy (or designate)

On a monthly basis the Manager, Privacy (or designate):

- Reviews specific PI data elements for each DtC service with stakeholders.
- Ensures location of PI accommodates easy retrieval, that PI is date stamped with initial collection and any updates.
- Reviews DtC services document to verify accuracy and currency of PI, including consumer verification.

12 RETENTION, TRANSFER AND DESTRUCTION OF CONFIDENTIAL INFORMATION

12.1 PURPOSE

The purpose of this policy and its 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.
- Fair Information Practices (FIPs) as detailed by the Office of the Privacy Commissioner of Canada (OPC) in their Privacy Toolkit.
- OTN policies, including OTN's privacy policies.

12.2 SCOPE

This policy applies to all OTN individuals (staff, contractors, students and volunteers) who have paper and/or electronic confidential information in their custody or control.

12.3 POLICY

OTN is committed to respecting individual privacy and to safeguarding and ensuring the security of confidential information. To fulfill this commitment, OTN has implemented privacy practices and procedures, including the retention, transfer and disposal guidelines detailed below, that adhere to the provisions of all applicable laws and guidelines.

12.4 RESPONSIBILITY

Manager, Privacy (or designate) in coordination with the Information Security Manager.

12.4.1 General Retention Guidelines

Personal information (PI) and personal health information (PHI) must be de-identified, where possible, to protect patient and consumer privacy. Records containing PI and PHI receive the highest level of protection in accordance with relevant policies and legislation, including OTN's general Privacy Policy, FIPs, and PHIPA.

As an agent of a HIC, electronic Service Provider (ESP) and as a Health Information Network Provider (HNIP) under PHIPA, OTN hosts and retains PHI on behalf of Health Information Custodians (HICs). PHI may only be retained in accordance with OTN's Retention and Sanitization Schedule which ensures compliance with legal data retention requirements, OTN's Privacy Policy and HIC requirements, where applicable.

As the manager of consumer PI collected from OTN's Direct to Consumer (DtC) services, OTN retains PI in accordance with OTN's Retention and Sanitization schedule, with exceptions related to legal requirements and/or if related to a current or anticipated claim, or a dispute. The length of retention is set to allow a consumer to obtain information after a decision and pursue redress. OTN does not retain and securely disposes of consumer PI that does not have a specific purpose or no longer fulfills its initial purpose (e.g. in the event of a Direct to Consumer service ending).Consumer PI collected by OTN will be stored in a secure database separate and apart from PHI and member data.

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 OTN individuals 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.

12.4.2 General Transfer Guidelines

Where permitted, transmission of PHI, consumer PI and/or 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 managed in accordance with OTN's Information Classification Policy and the Policy and Procedure for Facsimile Transmission of Confidential Information, where applicable. Such records must be securely stored and remain in the custody and control of the individual at all times in accordance with this policy.

OTN may transfer confidential information to a third-party for retention. 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. See Section 17 of the OTN Integrated Privacy Policy Framework for contracting requirements where consumer PI is transferred to third parties.

12.4.3 General Disposal Guidelines

Electronic and paper records containing confidential information must be disposed of securely. At OTN, secure disposal of paper records of consumer PI and/or PHI occurs only via third-party providers (as described below). The following elements must be documented in agreements with third parties providing secure disposal of records of confidential information in paper or electronic form, per OTN's policy on the execution of third-party agreements:

- The manner for securely transferring, retrieving and/or disposing of the records.
- The conditions pursuant to which the records will be transferred, retrieved and/or disposed of.
- The appropriate standard to be used for the disposal of confidential materials including paper records or electronic media (e.g. paper should be cross-cut shred to a standard of 3/8" maximum).
- OTN stakeholders or agent(s) responsible for ensuring the secure transfer, retrieval and/or disposal of the records.
- Date, time and mode of transfer of the records.
- Requirements for maintenance of a detailed inventory of transferred and retrieved records.
- Requirements for written confirmation to OTN for receipt of confidential records.
- Requirements for 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.
- A commitment to confidentiality by the third-party provider.

Certificates of destruction must be provided in accordance with the terms of the third-party agreement and filed by Records and Policy Management Specialist.
Third-party service providers engaged by OTN to destroy confidential materials must be bonded and insured.

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

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.

12.5 PROCEDURES

12.5.1 Retention of Personal Health Information

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

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

12.5.2 Transmission of Confidential Records

Refer to the security Policies and Procedures for Sending/Receiving Personal Information, Personal Health Information and De-Identified Health Information and Data Protection - Encryption, Transmission and Storage

12.5.3 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 erasure 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 employees to ensure confidential records are deposited in the confidential waste shredding bins for secure disposal. If an employee notices that confidential materials are not securely disposed of, he/she must report non-compliance with this policy immediately to the Manager, Privacy (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.

12.5.4 Retention/Disposal Schedule

OTN maintains a records retention schedule.

13 SAFEGUARDS

13.1 PURPOSE

To protect the Personal Information (PI) collected through Direct to Consumer (DtC) services, independent of format, from loss, theft, misuse (e.g., rogue access, disclosure, use, modification/tampering) to prevent harm to the consumer using the team and self-managed virtual care services accessible at otn.ca/patients.

13.2 POLICY

OTN follows its security policy framework with respect to the protection of PI in its control. OTN provides data protection for PI that is proportional to the likelihood and severity of possible harms.

13.3 RESPONSIBILITY

Manager, Privacy (or designate), in coordination with the Information Security Manager (or designate).

13.4 PROCEDURES

OTN follows its Security Policy and Procedures, which include:

- Assessing the harm to consumers in the event of accidental or deliberate loss, misuse, alteration or destruction of PI and protecting PI to an extent that matches or exceeds the potential harms.
- Reviewing physical controls (office access), technological controls (provisioning, encryption), organizational controls (security clearances) legal controls (contractual arrangements with third parties), which are commensurate with the characteristics and sensitivity of the information.
- Undertaking periodic security safeguard reviews to ensure adequacy and currency to address emergent vulnerabilities.
- Offering periodic, mandatory, staff security and privacy training regarding the management of PI and confidential information.

14 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 the OTN Human Resources, Privacy and Security teams, 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, voice mail messages, or MS Teams messages sent or received.

15 PRIVACY TRAINING AND AWARENESS

15.1 PURPOSE

The purpose of this policy is to create a prescriptive set of process and procedures, aligned with applicable OTN privacy and information security policies and standards, to ensure that a consistent and regular training and awareness program is in place, maintained and delivered to relevant individuals in order to ensure that individuals possess and demonstrate sufficient knowledge of privacy and information security in order to perform their functions in a compliant and risk aware manner.

This policy and procedure establishes the minimum requirements for the privacy and information security awareness and training controls.

15.2 POLICY

Privacy and information 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 privacy and security training within the first four weeks of employment/engagement. THERE ARE NO EXCEPTIONS TO THIS POLICY. Enhanced privacy training is mandatory for agents engaged in specialized areas such as project management and member services. Additionally, a privacy refresher training module must be completed by all agents annually.

Awareness and training content will be regularly reviewed by the Manager, Privacy (or designate) and Information Security Manager (or designate) and updated as appropriate. Awareness and training will include content from the privacy and information security policies in addition to legislative requirements and best practices.

All agents must sign an OTN confidentiality agreement and annually re-sign this agreement within the first forty-five days of each fiscal year. Additionally, third party contractors and vendors sign non-disclosure agreements, or agree to equivalent privacy clauses in a services agreement as necessary, prior to conducting work for OTN. Compliance is enforced by the VP Finance and Administration (or designate).

15.3 RESPONSIBILITY

The Manager, Privacy (or designate) and Information Security Manager (or designate) will ensure completion of privacy and security training by all agents within applicable timelines.

15.4 PROCEDURES

OTN designates the Manager, Privacy (or designate) and the Information Security Manager (or designate), as jointly responsible for preparing and delivering the privacy and security training. In instances where the training content has changed substantially, it must be approved by the VP Finance and Administration and VP Technology and Services respectively.

Privacy and information security staff will train and orient agents using an appropriate combination of in-person orientations and online eTraining materials, as well as posters, newsletters, iConnect announcements, events and guidelines for particular OTN services, supplemented by information specific to individual roles.

Successful completion of training will be established through a test to demonstrate essential privacy and security knowledge. The presenters providing the training will promote an interest in privacy and security knowledge. Privacy and security staff 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.

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

1. Managers and Human Resources notify the Manager, Privacy (or designate) concerning new hires commencing employment at OTN.
2. Privacy and/or Security office staff provide privacy and related security training using various formats such as e-modules, in-person sessions or presentations. The Privacy and Security teams will choose the appropriate training format based on the audience and content to be delivered.
3. In addition, written materials (OTN Privacy Policy, OTN FAQ, OTN Security Policy and Acceptable Use Policy) are provided to new agents.
4. The OTN confidentiality agreement is signed by the agent.
5. The OTN confidentiality agreement is retained in the employee file.

The privacy and security training includes:

- OTN's status under PHIPA and the duties and responsibilities that arise as a result of this status.
- Definitions for personal and personal health information (PI/PHI) and instructions for agents on how to identify and appropriately handle such information.
- The particular privacy responsibilities stemming from offering team and/or self-managed virtual care service to consumers.
- Limitations placed on access to and use of PI/PHI held by OTN.
- Instruction for agents to direct any access requests, including for PI/PHI, to the OTN Privacy Office.
- 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, procedures, standards, guidelines and practices.
- An overview of the privacy and security programs, team structure and key program components.
- 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.
- An outline of the OTN Privacy Breach Management Policy, which includes the procedures for identifying, reporting and containing a privacy breach, as well as the duties and responsibilities, which are imposed on agents to identify, report, and contain the breach, to participate in the investigation and assist as requested in remediation of both privacy breaches and information security breaches.

Annual privacy refresher training modules and privacy awareness training/campaigns may include the content below, where applicable:

- Role-based training relating to an agent's day-to-day duties.
- Any new privacy and security policies, procedures, standards, tools, guidelines and practices.
- Significant amendments to existing privacy and security policies.
- Changes made to training modules and/or updates based on recommendations from privacy impact assessments, 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 assessments, privacy audits and the investigation of privacy breaches and privacy complaints.

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

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 (or designate) will provide timely privacy information to staff and managers on identified outstanding privacy issues and mitigation plans. This will be communicated through presentations to affected agents, correspondence, newsletters, and/or postings on OTN's iConnect.

A breach of OTN's privacy or security policies may result in disciplinary action, up to and including termination.

15.5 Privacy and Security Training Attendance Logs

To ensure compliance with mandatory training requirements, and in accordance with OTN's Privacy Training and Awareness Policy, OTN maintains a log to track attendance/completion of privacy and security training.

The log is the responsibility of the Manager, Privacy (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

- Completion dates
- Test scores
- Confidentiality agreement status

16 LIMITING AGENT ACCESS TO AND USE OF PERSONAL AND PERSONAL HEALTH INFORMATION

16.1 PURPOSE

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

16.2 POLICY

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

Access to personal and 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 or personal health information except as necessary for his or her employment or contractual responsibilities.

OTN agents are required to only 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 or 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.

16.3 RESPONSIBILITY

Manager, Privacy (or designate)

16.4 PROCEDURE

All agents, including employees, consultants, contractors and seconded employees, must apply to the Manager, Privacy (or designate), for approval to access and use personal and/or 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

Access levels will be granted based on an evaluation of multiple factors including, but not limited to, whether the job role requires the ability to:

- Read/view PHI/PI
- Use PHI/PI
- Disclose PHI/PI
- Delete PHI/PI

The Data Access Form must be signed by the immediate supervisor of the agent and forwarded to the Manager, Privacy (or designate), along with a copy of the job specifications or contract.

The Manager, Privacy (or designate), considers the following criteria when reviewing the application for approval:

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

If the Manager, Privacy (or designate), denies access, the Manager, Privacy (or designate), notifies the agent and his/her supervisor in writing with an explanation of the reasons.

Where the Manager, Privacy (or designate), approves an application, the Manager, Privacy (or designate), forwards to the agent's supervisor and the relevant System Administrator a request including the following:

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

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

The Manager, Privacy (or designate), ensures that all agents sign confidentiality agreements before being given access to personal and/or personal health information.

16.4.1 Notification and Termination of Access and Use

The supervisor of agents granted approval to access and use personal and/or personal health information must notify the Manager, Privacy (or designate), and relevant 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 use required by the agent.

The written notification sets out:

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

The relevant OTN System Administrator terminates/modifies agent access on the date specified and updates a log of agents granted approval to access/use/disclose personal and/or personal health information (see section 16.5 of the OTN Integrated Privacy Policy Framework).

16.4.2 Document Retention

The Manager, Privacy (or designate), is responsible for securely maintaining all files relating to agent access and use of personal and/or 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 relevant System Administrator securely maintains the log of agents granted approval to access, use, or disclose personal and/or personal health information.

16.5 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)

16.6 Related Documents

Records Management Policy

17 EXECUTING AGREEMENTS WITH THIRD-PARTY SERVICE PROVIDERS

OTN enters into legal agreements with third parties for the provision of goods and services. The following section outlines contracting with third parties and should be used as guidance for specific agreements with Health Information Custodians (HICs). For clarity, any reference to the term 'agreement' is used in an illustrative manner and not specific to the term agreement proper and should be read to be inclusive of any legal instrument executed between OTN and a third-party service provider.

17.1 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 Ontario Information and Privacy Commissioner with respect to the protection of personal health information (PHI).

To ensure that OTN executes agreements with third-party service providers, where consumer Personal Information (PI) is collected, based on the policies and procedures detailed in the Fair Information Principles as set out in the OTN Integrated Privacy Policy Framework.

17.2 POLICY

A written agreement must be entered into with third-party service providers prior to permitting access to and use of PI and/or PHI including:

- Those that are contracted to retain, use, transfer or dispose of records of PI and/or PHI.
- Those that are contracted to provide services to use electronic means to collect, use, modify, disclose, retain or dispose of PHI (electronic service providers).

Where consumer PI and/or PHI will be transferred to a third-party the following are required within or leading to any service agreement:

- Point of accountability to handle all privacy aspects of contract.
- Statement of use limitations for third party.
- Disclosure limits set on third party.
- Contact information for consumers seeking access to their PI and/or PHI.
- Return and disposal protocols upon completion of third-party contract.
- Statement of security measures applied to the protection of consumer PI and/or PHI.
- Audit protocols to allow OTN to audit for contract compliance.

17.3 RESPONSIBILITY

Manager, Privacy (or designate)

17.4 PROCEDURE

17.4.1 Third-Party Service Provider Agreement Initiation

Third-party service providers are engaged by OTN's Contracts & Legal Team to enter into agreements based on OTN procurement policies.

1) The Procurement team, in consultation with the Contracts & Legal Team, will engage the Manager, Privacy (or designate) during the drafting of any procurement documents to ensure the appropriate privacy language is included in the tender documents, including any legal terms contained therein.

2) Upon identification of a third party service provider with whom OTN wishes to contract, OTN's Contracts & Legal Team will engage with the Manager, Privacy (or designate), for completion of a third-party service agreement (such agreement can be a negotiated agreement or from a template disclosed through the procurement tender). The Contracts & Legal team will include the following information, as available:
   a) A description of the task to be performed by the third party.
   b) A copy of the procurement tender or statement of work.
   c) A copy of the successful proposal.
   d) Type and level of personal and/or personal health information to which the third party will be given access, including timeframe.
   e) Why the function cannot be performed with de-identified and/or aggregate data.
   f) When provided, personal and/or personal health information will be securely destroyed from OTN server at end of the agreement term and after purpose for collection, use and disclosure is no longer required.

3) The Manager, Privacy (or designate), provides all appropriate privacy clauses (and any documentation to be incorporated by reference) to be included in the agreements with Third-Party Service Providers, and forwards it to the Director, Legal and Regulatory Affairs (or designate) for approval.

4) Authorized signatory(ies) of OTN execute the third-party service provider agreement; the Contracts & Legal Team then provides a copy of the signed agreement to each of the third-party service provider and the Manager, Privacy (or designate).

5) The Manager, Privacy (or designate) updates a log of agreements with third-party service providers with the following information provided by Privacy Specialist responsible for the project, program or initiative:
   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.
   e) Where information is removed, and destruction of the information is required, the Manager, Privacy (or designate) flags the disposal date for follow-up.

17.4.2 Changes to Third-Party Service Agreements

The Contracts & Legal Team must notify the Manager, Privacy (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 (or designate) informs the Director, Legal and Regulatory Affairs (or designate) of any such changes and upon acknowledgement of same, the Manager, Privacy (or designate) will update the log of agents granted approval to access/use/disclosure of personal health information.

Where privacy provisions have significantly changed after the agreement has been originally executed, and where the collection, use and disclosure of personal information and/or personal health information, or access to same, have substantially changed; the Manger, Privacy (or designate) informs Contracts & Legal Team in writing to enact changes to third-party service agreement.

17.4.3 Disposal/Destruction of Personal and/or Personal Health Information

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

If the third party is found to be in breach of its contractual obligations, as it relates to disposal/destruction, and action is not taken to remedy same as permitted by the agreement, the Manager, Privacy (or designate) may instruct the Contracts & Legal Team to take all measures authorized by the agreement. The Manager, Privacy (or designate) may notify the Information and Privacy Commissioner that the third party is in breach and where appropriate lodge a complaint.

17.4.4 Document Retention

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

- Key correspondence from the Contracts & Legal Team
- Third-party service provider agreement
- Log of agreements with third-party service providers

17.4.5 Template for Third Party Service agreement

Available on demand.

18 PRIVACY IMPACT ASSESSMENTS

18.1 PURPOSE

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

According to the Regulation, OTN acts as a HINP when it provides services to two or more health information custodians 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)]
This policy also provides guidance related to privacy impact assessment (PIA) requirements for consumer-based health services.

18.2 SCOPE

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

18.3 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. Additionally, privacy impact assessments may be used to ensure alignment with Privacy by Design principles.

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 for 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 and other funding partners.

For initiatives involving consumer-based health services, where only PI is held by OTN, OTN will conduct a privacy impact assessment or privacy review for any new technology and/or service, or new use of PI where PI is planned for collection,

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 an initiative will require a full privacy impact assessment, an update (or 'delta') to an existing privacy impact assessment, or other privacy assurance services, such as an abridged privacy review or consulting services.

OTN must undertake privacy impact assessments or abridged privacy reviews[3]:

- On existing programs (including pilots, projects, demonstration projects and proofs of concept), 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 of 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 and/or personal health information.
- On any other program, processes and/or system change with privacy implications.

Privacy impact assessments will be reviewed by the OTN Privacy team every three years to ensure that the assessments remain up to date. OTN will expire privacy impact assessments where a more recent assessment of the service has been completed. Where updates to an existing assessment are required to ensure that the assessment accurately captures any collection, use, disclosure, retention or destruction of PHI and/or PI in relation to the service, OTN will supplement the existing assessment. OTN will not change the content of the original assessment. Where significant changes have occurred, including where there has been a significant change to the technology, vendor/partner (where applicable) or to functionality, OTN will initiate a new assessment and determine the most appropriate risk assessment tool.

Privacy impact assessments are not required where 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 or other relevant team prior to launching or going live with any

[3] Determination of whether to do a full assessment or review is based on using a preliminary privacy risk assessment checklist to assess the scope and severity of risk.

initiative, program or service. Any exception to this rule must be reviewed/approved by an SLT, Program Lead or Executive Sponsor in consultation with the Manager, Privacy (or designate).

18.4 RESPONSIBILITY

Manager, Privacy (or designate).

18.5 PROCEDURE

The Manager, Privacy (or designate) participates in OTN's project gating process and evaluates the need for a privacy impact assessment in relation to new and/or changed programs, services, systems and technologies. In the case of new programs or changes to existing information systems or technologies involving personal and/or personal health information, the Manager, Privacy (or designate) conducts a privacy impact assessment as early as possible in the project lifecycle. This ensures that privacy protections are designed into the new system or, in the case of changes to an existing system, the proposed system enhancements or features. The PIA may be revisited throughout the project lifecycle to ensure that the assessment provides an analysis of all elements, features and enhancements included in the project. All risks and recommendations resulting from the PIA are documented and tracked in a workplan, ensuring that all risk mitigation activities are undertaken in accordance with project timelines.

Where the privacy impact assessment is being outsourced, the Manager, Privacy (or designate) completes a request for authorization (RFA), drafts a statement of work, initiates a request for proposal process, executes internal sign-off for 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 (or designate), the Manager, Privacy (or designate) leads the privacy impact assessment process.

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

The Manager, Privacy (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[4] or, where only PI is involved, Canada's Office of the Privacy Commissioner's PIA toolkit[5]. The Manager, Privacy (or designate), ensures that the content of the privacy impact assessment includes:

- Information system, technology or program under assessment.
- Nature and type of personal and/or personal health information collected, used or disclosed.
- Sources of the personal and/or personal health information.
- Purpose of the collection use or disclosure.

[4] https://www.ipc.on.ca/wp-content/uploads/resources/phipa_pia-e.pdf
[5] https://www.priv.gc.ca/en/privacy-topics/privacy-impact-assessments/gd_exp_201103/

- Reason that personal and/or personal health information is required for the purposes identified.
- The flows of personal and/or personal health information.
- Statutory authority for each collection, use and disclosure of personal and/or personal health information.
- Limitations imposed on the collection, use or disclosure of the personal/and or personal health information.
- Whether or not the personal and/or personal health information is or will be linked to other information.
- Retention period for the personal and/or personal health information.
- Secure manner in which the records of personal and/or personal health information will be retained, transferred and disposed of.
- Functionality for logging access, use, modification and disclosure of the personal and/or 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 and/or personal health information.
- Risks to the privacy of individuals whose personal and/or personal health information is or will be part of the information system or technology, and an assessment of risks.
- Recommendations to address, eliminate or reduce the privacy risks identified.
- Any threat risk assessments (TRAs) that have been completed.
- Any reference documentation.
- The identity of team members and contributors.

The Manager, Privacy (or designate) submits the findings of the completed privacy impact assessment and recommendations to the Director, Legal and Regulatory Affairs or other relevant team for review. The risks to OTN and an action plan with timeframes and required resources are submitted for review to the relevant teams and/or Executive Sponsor where appropriate.

With the approval of the relevant teams and/or Executive Sponsor, the Manager, Privacy (or designate), coordinates implementation of the recommendations arising from the privacy impact assessment by:

- Developing work plans to address risks as identified in the privacy impact assessment and communicating the work plan to the project team.
- Assigning action items in consultation with the project or other relevant team to the appropriate project or other relevant team member or stakeholder in the organization.
- Providing advice, recommendations and support to business areas for 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 (or designate) develops and maintains a log of privacy impact assessments.

The Manager, Privacy (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 and internal and external stakeholders.
- Where appropriate, posts all relevant privacy impact assessments on the OTN websites.
- Tracks and monitors, through regular reviews, completed privacy impact assessments to ensure their currency.
- Ensures appropriate policy, communication and training plans are in place to support compliance with this policy and related procedures.

The Manager, Privacy (or designate), 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 of OTN's Privacy & Security Lateral Team and Executive Sponsor as required to conduct and act on the results of the privacy impact assessment process.
- Presents high and medium risks to OTN's Director, Legal and Regulatory Affairs for review and discussion of mitigation plans.

18.6 Document Retention

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

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

18.6.1 Log of Privacy Impact Assessments

Log contents should include:

- Date the PIA was last updated
- The vendor who completed the PIA (where applicable)
- Confirmation that the PIA was completed internally (where applicable)

19 PRIVACY COMPLAINTS

19.1 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.

19.2 POLICY

Any member of the public may challenge OTN's compliance with its 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 where PI and/or PHI is involved and how to do so.

OTN will also ensure that the general public is aware of the process for forwarding a privacy complaint involving consumer-based health services available through OTN.ca.

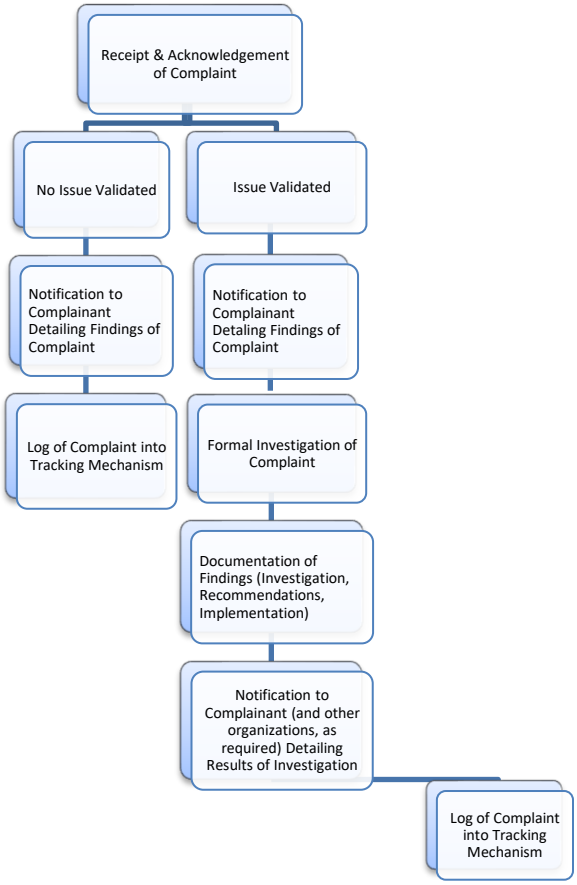
OTN will acknowledge privacy complaints in a timely manner and generally within two business days of the submission of the complaint, provided that the complaint is accompanied by accurate contact information of the complainant.

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.

19.3 PROCEDURE

19.3.1 Privacy Complaint Management Process

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



19.3.2 Receipt of Complaint

Information regarding the process for making a privacy complaint is publicly available on OTN's website at https://otn.ca/ here.

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

OTN's website will also indicate that complaints regarding OTN's compliance with PHIPA and its regulation or with Fair Information Practices can be made 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 will be received and acknowledged by OTN and referred to the Manager, Privacy 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.

19.3.3 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 or validity of the complaint into one of the following categories:
  - No issue validated
  - Issue validated
- All complaints, where PHI has been compromised are considered a high-risk complaint.
- 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. The Manager, Privacy, 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 19.3.5 of the OTN Integrated Privacy Policy Framework for responding to a complainant where an investigation will be conducted.

If a complaint is found to be minor, the Manager, Privacy will attempt to achieve an informal resolution without a formal investigation. See section 19.3.4 of the OTN Integrated Privacy Policy Framework 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.

19.3.4 Notification to Complainant Detailing Non-Investigation

In situations where a complaint will not be investigated, a written response, approved by the Manager, Privacy 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.

19.3.5 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 Manager, Privacy or an appropriate VP 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 (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 Privacy Office 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 for PHIPA related issues.

For complaints related to OTN's shared information or Direct to Consumer services, the Manager, Privacy, will respond and outline any protocol for consumer complaints.

19.3.6 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 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 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 Manager, Privacy will provide a written report of the investigation to OTN's Board of Directors including recommendations for remediation.

19.3.7 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 Manager, Privacy 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.

19.3.8 Notifications

The Manager, Privacy 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.

19.3.9 Complaint Log and Tracking Mechanism

The Manager, Privacy 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.

19.4 RESPONSIBILITY

Manager, Privacy (or designate)

20 PRIVACY REQUEST TO ACCESS OR CORRECT PI AND/OR PHI IN OTN CONTROL

20.1 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 and, in adherence to FIPs.

20.2 POLICY

Any member of the public may request access to their PI and/or PHI or to correct their PI and/or PHI OTN will ensure there is a mechanism for informing the general public and users of OTN's shared information and Direct to Consumer Services 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 request provided that the request is accompanied by accurate contact information of the complainant.

20.3 RESPONSIBILITY

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

20.4 PROCEDURE

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

- Access Request for Your Information
- Request for Correction to Information

For PI held in relation to OTN's shared information or Direct to Consumer services, the Manager, Privacy (or designate):

- Reviews shared information and DtC services documentation and processes for consumer ease of access to their PI.
- Reviews PI access responses to ensure the PI is without acronyms, abbreviations or codes to ensure readability.
- Reviews OTN's shared information and DtC services correction and amendment processes for consumer PI.

- Reviews supporting documentation where disagreements on PI accuracy occur, or where reasons for not providing access arise.
- Reviews disclosure of corrected or amended PI to 3rd parties that are authorized to use consumer PI.
- Reviews record of access requests, the 30-day response times and, where exceptions occur, determines the validity of delays for the Annual Privacy Report.
- Reviews written responses to consumers where PI was not made accessible and includes summary in the Annual Privacy Report.
- Provides training and education to staff responsible for responding to access requests.

21 PRIVACY AUDITS AND MONITORING REVIEWS

21.1 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.

21.2 POLICY

21.2.1 Summary

OTN considers all PI and/or PHI in its custody to be highly sensitive and implements appropriate safeguards to protect the privacy of individuals whose PI and/or PHI is received and to maintain the confidentiality of that information. Steps are taken to protect PI and/or PHI against theft, loss and unauthorized use or disclosure, and to protect records of PI and/or 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.

21.2.2 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 PI and/or 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 and/or PI 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 and/or PI 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. Through regular touch points, OTN Privacy Specialists provide up to date snapshots to the Manager, Privacy, to detail progress against annual privacy priorities and ensure timely review of any areas of concern.

21.2.3 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 and PIPEDA;
- Orders, guidelines, fact sheets and best practices issued by the Information and Privacy Commissioner of Ontario (IPC) and Canada's Office of the Privacy Commissioner;
- 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 and PIPEDA;
- 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, medium or low risk operational areas [NTD: reference OTN Corporate Risk Management Policy] governed by internal documentation (policies, procedures and guidelines).

21.2.4 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.

21.2.5 Persons Responsible for the Privacy Audits and monitoring reviews

The Manager, Privacy (or designate) will assume primary responsibility for the privacy audit and monitoring reviews.

21.2.6 Timing of Privacy Audits and Monitoring reviews

Privacy audits will be conducted as required. The frequency of the privacy audit will occur at the direction of the Manager, Privacy as well as ad hoc audits required for cause, or at the request of the SLT 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.

21.2.7 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 Manager, Privacy (or designate).

Monitoring reviews will be submitted in the privacy annual report.

21.3 RESPONSIBILITY

Manager, Privacy (or designate)

21.4 PROCEDURE

21.4.1 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 (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 (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 and/or PI. As per the terms of the third-party service agreement, the third-party will provide the Manager, Privacy (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 (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 (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 (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 Director, Legal and Regulatory Affairs through inclusion of a summary in the annual privacy report.

21.4.2 Addressing Recommendations from an Audit or Review

Outcomes of the privacy audit, including all recommendations, will be addressed by the Manager, Privacy (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 Privacy Office in consultation with applicable OTN staff where required.

The Privacy Office 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 Privacy Office 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 Manager, Privacy (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.

21.4.3 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 Manager, Privacy (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.

21.4.4 Communication of Findings from an Audit or Review

The Manager, Privacy (or designate) will ensure that a report of relevant findings and recommendations from each privacy audit or monitoring review is provided to the OTN Planning and Priority Committee of the 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 PI and/or PHI including the IPC, the Ministry of Health and Long-Term Care, OTN and the public.

21.4.5 Retention of Privacy Audit Documentation

The Manager, Privacy (or designate) will retain copies of the reports, which will be made available to the OTN Planning and Priority Committee of the 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 Manager, Privacy (or designate) or Information Security Manager in accordance with OTN's Privacy Breach Management Policy.

22 PRIVACY BREACH MANAGEMENT

22.1 PURPOSE

This Privacy Breach Management Policy and Procedure provides guidance to OTN employees, students, consultants and other individuals on the appropriate steps to take in the event of a privacy incident or breach. This includes defining roles and responsibilities and documenting notification protocols to affected individuals, health information custodians and the Ontario Information and Privacy Commissioner, as appropriate.

This policy and its procedure set out the points of responsibility within OTN to ensure a rapid and effective response in the event of a privacy incident or breach involving personal health information (PHI) and/or personal information (PI) in OTN's telemedicine environment or a shared information/Direct to Consumer (DtC) service. It also documents best practices to monitor, report, contain, notify, investigate, and remediate an incident.

22.2 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 (referred to in this policy as OTN Individuals) must comply with the applicable sections of this policy as a condition of continued employment or engagement.

22.3 POLICY

22.3.1 Duty of OTN Individuals to Report Privacy Incident

Any OTN Individual who becomes aware of a privacy-related incident involving PHI and/or PI has the duty to report that incident as soon as practically possible to OTN's Privacy team at privacy@otn.ca. 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, remediation and response.

Upon discovery of an actual or potential privacy incident involving PHI or PI, OTN shall act immediately to contain the incident to prevent further damage (see section 22.6.3 of the OTN Integrated Privacy Policy Framework on containment).

Depending on the scope and severity of the privacy incident or breach, the OTN Manager, Privacy (or designate) may escalate the incident details to the OTN SLT in accordance with OTN's escalation process.

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

22.3.2 Identifying a Privacy Incident or Breach

In OTN's Telemedicine Environment

A privacy incident involving PHI/PI in OTN's telemedicine environment occurs when anyone who has cause to work for or with OTN:

- Has contravened or is about to contravene a provision of PHIPA or its Regulations.
- Collects, uses or discloses PHI and/or PI in a telemedicine environment for purposes other than those described in their roles & responsibilities, agreements and/or policies.
- Believes or has reason to believe that PHI and/or PI has been lost, stolen, used, disclosed, copied or modified in an unauthorized manner.
- Provides access to PHI and/or PI in a telemedicine environment to an individual who is not otherwise permitted to access the data.
- Accesses PHI and/or PI in a telemedicine environment without authority to do so.
- Contravenes a requirement relating to the handling of PHI and/or PI as set out in OTN's Confidentiality Agreement with which the user has agreed to comply.

In OTN's Shared Information and Direct to Consumer Services

A privacy incident involving PI in the context of an OTN shared information or DtC service occurs when anyone who has cause to work for or with OTN:

- Collects, uses or discloses PI in a shared information/DtC service in a manner that clearly violates the Fair Information Principles (FIPs).
- Collects, uses or discloses PI in a shared information/DtC service for purposes other than those described in their roles & responsibilities, agreements and/or policies.
- Believes or has reason to believe that PI has been lost, stolen, used, disclosed, copied or modified in an unauthorized manner.
- Provides access to PI in a shared information/DtC service to an individual who is not otherwise permitted to access the data.
- Accesses PI in a shared information/DtC service without authority to do so.
- Contravenes a requirement relating to the handling of PI as set out in OTN's Confidentiality Agreement with which the user has agreed to comply.

22.3.3 Notification

For Breaches Occurring in OTN's Telemedicine Environment

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/or other applicable stakeholders as required at the first reasonable opportunity. The applicable HIC will notify impacted individuals as required under PHIPA.

Further details regarding incident notification by OTN are provided under section 22.6.5 of this document (pg. 74).

For Breaches Occurring in OTN's Shared Information and Direct to Consumer Services

Where there is a privacy breach of PI in OTN's shared information or DtC services in accordance with the Fair Information Principles or OTN's agreements or contracts, OTN will notify all applicable vendors and partners where appropriate at the first reasonable opportunity. OTN will notify affected individuals where it has been determined that the breach resulted in a "real risk of significant harm" to those individuals. Further details regarding incident notification by OTN are provided under section 22.6.5 of this document (pg. 74).

22.4 Responsibility

Manager, Privacy (or designate) and Information Security Manager (or designate).

22.5 Roles and Responsibilities

OTN Individuals

Regardless of the service offering involved, all OTN Individuals must immediately report actual and potential incidents and breaches involving PHI and/or PI to the OTN Privacy team, via email to privacy@otn.ca, or to the Information Security Manager. OTN Individuals must contain the incident or breach if capable of doing so, in full cooperation with the Manager, Privacy (or designate), and the Information Security Manager (or designate).

OTN's Telemedicine Environment

OTN

In the context of OTN's telemedicine environment, OTN functions as an "agent," and as a "health information network provider" ("HINP") under PHIPA. Therefore, it is required to notify 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 to allow hospitals and other applicable stakeholders to comply to their obligations under PHIPA and the Freedom of Information and Protection of Privacy Act (FIPPA).

OTN's Manager, Privacy, and Information Security Manager, or their delegates, in consultation and collaboration with all applicable HICs and other applicable stakeholders, will launch and lead privacy breach investigations and incident management processes when they become aware of an actual or potential privacy breach.

Members & External Stakeholders

OTN members, 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.

OTN's Shared Information & Direct to Consumer Services

OTN

With respect to its shared information and DtC services, including those services available on www.otn.ca/patients, OTN does not directly fall under the scope of the Personal Health Information Protection Act (PHIPA) or the Personal Information Protection and Electronic Documents Act (PIPEDA). However, OTN follows industry best practices with respect to the protection of personal information as documented in the Canadian Standard Association's "Model Code for the Protection of Personal Information" (the Fair Information Principles or FIPs) which are foundational to PIPEDA and applicable Canadian privacy legislation. OTN will similarly follow industry-standard approaches to incident management with respect to incidents involving PI in OTN's shared information or DtC services.

OTN Partners and Vendors

OTN partners and vendors are made aware of how to recognize privacy incidents and breaches in a shared information/DtC service. Partners and vendors are also made aware of their responsibility to notify OTN as soon as reasonable possible in the event of a privacy incident or breach through their agreements with OTN.

22.6 PROCEDURES

22.6.1 Monitoring for Incidents

OTN, healthcare organizations, partners, vendors and other stakeholders must monitor their activities to ensure PHI and/or PI is collected, used, and disclosed within the permitted scope of 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 individuals with access to the OTN telemedicine environment and shared information/DtC services 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
- Receiving, investigating and reporting on privacy incidents and/or complaints made by HICs, clients, the public, and other stakeholders.

22.6.2 Reporting Incidents to OTN

OTN Individuals

Regardless of the service offering involved, OTN Individuals must immediately report privacy incidents or suspected privacy incidents involving PHI or PI to the OTN Privacy team at privacy@otn.ca.

Depending on the scope and severity of the privacy incident or breach, the OTN Manager, Privacy (or designate) may escalate the incident details to the OTN SLT in accordance with OTN's escalation process.

OTN's Telemedicine Environment

OTN Members & External Stakeholders
OTN members and external stakeholders must immediately report all confirmed or suspected privacy incidents or breaches involving PHI or PI in OTN's telemedicine environment to the OTN Privacy team at privacy@otn.ca.

OTN's Shared Information and Direct to Consumer Services

OTN Partners and Vendors
OTN partners and vendors must immediately report all confirmed or suspected privacy incidents or breaches involving PI in OTN's shared information/DtC services to the OTN Privacy team at privacy@otn.ca.

22.6.3 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 and/or PI from being affected and ensuring that affected records are not further compromised.

OTN may use any of the following measures, alone or in combination, to contain privacy incidents or breaches involving PI or PHI:

- 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 if the incident occurs in OTN's telemedicine environment
- Temporarily disabling webcast archiving for specific webcasts if the incident occurs in OTN's telemedicine environment
- Determining the need for a team to further assess problem(s) in detail
- Determining initial communication strategy and escalating 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/PI that is the subject of the privacy incident and/or other PHI/PI is no longer at risk of inappropriate collection, use, disclosure or access.

22.6.4 Evaluation of Associated Risks

Once the privacy incident or 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 incident at the first reasonable opportunity and for gathering the following information:

- The date and time the incident occurred
- How and when the incident was discovered
- 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 22.6.3 and 22.6.6 of this Integrated Privacy Policy Framework)

Several factors are considered when assessing the severity of an incident or breach. The criteria used by the OTN Privacy team to assess incident/breach severity are documented in section 28.4, Table 1, of this Integrated Privacy Policy Framework.

The Privacy Team will document the results of the internal investigation in a *Privacy Investigation Summary*. *Privacy Investigation Summaries* include the following information:

- 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 (confirmed 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 SLT and the Board.

22.6.5 Incident Notification by OTN

OTN's Telemedicine Environment

Health Information Custodians

Where there is a privacy breach in accordance with PHIPA and/or FIPPA, OTN will notify all applicable health information custodians (HICs) and other appropriate stakeholders at the first reasonable opportunity. OTN will provide the applicable HICs with a description of the incident (including incident date and time), the containment and remediation efforts undertaken by OTN as of the notification date, the data elements impacted and the individuals to whom those data elements pertain in relation to the HIC.

Affected Individuals

Under PHIPA and FIPPA, it is not OTN's role to notify the individual(s) to whom the breached PHI or PI belongs. However, 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 breached.

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
- How to make a complaint to the IPC

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

Information Privacy Commissioner

OTN will report privacy incidents or breaches involving PHI to the Ontario Information and Privacy Commissioner (IPC) when OTN determines that notification to 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.

OTN's Shared Information and Direct to Consumer Services

OTN Partners and Vendors

Where there is a privacy breach of PI in relation to OTN's shared information and/or DtC services, OTN will notify applicable vendors and partners at the first reasonable opportunity. OTN will coordinate with its vendors and partners to contain, investigate and remediate all incidents and breaches involving PI.

Affected Individuals

OTN will notify affected individuals as soon as reasonably possible when there is a breach that creates a "real risk of significant harm", which can include reputational harm, to an individual. OTN determines if there is a "real risk of significant harm" by evaluating the criteria documented in section 28.4, Table 1, of this Integrated Privacy Policy Framework.

Notification will include:

- The date of the incident
- A general description of what happened
- A description of the 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 access credit or identity theft monitoring services)
- The contact information of an individual who can provide further information or assistance
- How to make a complaint to the Ontario Information and Privacy Commissioner (IPC).

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

Information Privacy Commissioner

OTN will report privacy incidents or breaches involving PI to the Ontario Information and Privacy Commissioner (IPC) when OTN determines that such notification is appropriate or required, assistance from the IPC is required to resolve the incident, or the incident may otherwise come to the attention of the IPC.

Other Notifications

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

- Law enforcement, if theft or another crime is suspected (e.g., identity theft).
- Vendors or suppliers that may need to assist in incident containment, resolution and prevention of future incidents.
- Professional or regulatory bodies responsible for disciplining individuals involved in the incident and/or that require notification.

22.6.6 Remediation of Privacy Breaches

The OTN 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.

22.6.7 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 (e.g., security policies, record retention and collection policies, etc.), with regular reviews continuing after the investigation ends.
- a review of employee training practices.
- a review of service delivery partners (e.g., HICs, contractors, service providers).

The OTN Privacy team will close privacy investigations upon completion of incident containment and investigation, and once recommendations for immediate action have been closed. Following the closure of an investigation, OTN will continue to track and monitor for completion and implementation of any additional recommendations.

22.7 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

OTN Privacy Investigation Severity Matrix

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

22.8 Related Documents

Subject	Number
Execution of Confidential Agreements by Agents	18.07.PP
Information Security Incident Response	21.43.P
OTN Integrated Privacy Policy Framework	
OTN Privacy Investigation Severity Matrix	
Privacy Breach Management Checklist	18.18.F2
Privacy Investigation log	
Summary of Privacy Investigation form	

23 TERMINATION OF EMPLOYMENT/CONTRACTUAL RELATIONSHIP

23.1 PURPOSE

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

The following privacy-related components are incorporated as part of OTN's broader termination policy and procedures.

23.2 POLICY

OTN has a Leaving the Organization Policy and exit procedures in relation to any agent terminations in instances where these parties had access to personal information or personal health information. Agents include all employees, contractors, volunteers, students and any other parties engaged in employment, contractual or other working relationships with OTN.

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 by Human Resources prior to leaving the premises. In the case of OTN employees or service providers who work remotely, arrangements are made to ensure the prompt return of OTN property to OTN in the event of a termination. OTN's Human Resources team is responsible for coordinating and managing the safe return of OTN property.

23.3 RESPONSIBILITY

Director, Human Resources (or designate)

23.4 PROCEDURES

Termination of employment, resignation and discharge procedure:

- The determination to discharge an agent from employment at OTN must be made in consultation with the Director, Human Resources (or designate) and communicated to the Manager, Privacy (or designate) as well as the Information Security Manager.
- The agent's leader will communicate to staff the departure/termination of identified agent(s) in accordance with broader OTN HR procedures.
- OTN ensures that all relevant policies and 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 Information Security Manager (or designate) at the time of notification of discharge, will coordinate with Human Resources and building management to cancel all access for the agent to OTN premises, to locations within the premises where records of personal health information are retained, printers, and to the information technology operational environment immediately upon termination or cessation of employment, contractual or other relationship;
- The Director, Human Resources (or designate) will log status of secured items access controls noted in this policy, and will also document and action any exceptions;
- The Director, Human Resources or delegate will follow-up directly within 2 business days with terminated parties to secure outstanding items and escalate as necessary. This includes coordinating with the Manager, Privacy to notify the IPC in the event of willful non-compliance and, with IPC guidance, seeking lawful means to retrieve unsecured items/information as deemed appropriate.
- Consequences for failing to comply with termination protocols are detailed in OTN employment/contracting agreements and such a failure will be treated as a privacy and security breach according to OTN's policies and procedures for privacy and security breach management.
- The Manager, Privacy (or designate) and the Information Security Manager will notify the Director, Human Resources at the first reasonable opportunity if an agent may have created or discovered a breach of this policy or its procedures.

24 EXECUTION OF CONFIDENTIALITY AGREEMENTS BY AGENTS

24.1 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.

24.2 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 24.1 of the OTN Integrated Privacy Policy Framework) 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 the first forty-five days of the start of OTN's fiscal year. External consultants and vendors providing services to OTN are bound by the privacy and confidentiality provisions included in service-level agreements.

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 Manager, Information Security or designate will be notified of anyone failing to sign their agreement by the Manager, Privacy (or designate). Upon receipt of notification the Manager, Security or designate will suspend all information access privileges until such time as the confidentiality agreement is signed.

24.3 RESPONSIBILITY

Director, 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.

24.4 PROCEDURES

The Leader (or designate) of each OTN department, as part of their job specifications, is accountable and responsible for ensuring that a confidentiality agreement is duly signed in the timeframes noted above for all staff, consultants and other individuals associated with their department. The Leader (or designate) is responsible for notifying the Director, 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.

In addition to signing the confidentiality agreement, OTN employees, consultants, students and other individuals are required to complete privacy and security training. The Manager, Privacy (or designate), will notify individuals by correspondence of the need for such training. Upon receipt of the notification, the OTN employees, consultants, students and other individuals to whom this applies must successfully complete the privacy and security training established by OTN. Successful completion will require a score of 80% or higher on a privacy quiz undertaken at the completion of the training.

The Director, Human Resources or designate will log and retain paper copies of signed confidentiality agreements. The Manager, Privacy or designate will notify by correspondence the responsible Director if any individual under that Director's auspices does not meet the timelines for signing confidentiality agreements.

Confidentiality agreements maybe subject to privacy audits by the Manager, Privacy or designate (see section 21 of this OTN Integrated Privacy Policy Framework). Any breach of conditions of the confidentiality agreement will be subject to the Policy and Procedures for Privacy Breach Management (see section 22 of this OTN Privacy Policy Framework).

25 DISCIPLINE AND CORRECTIVE ACTION INVOLVING AGENTS

25.1 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.

25.2 POLICY

OTN's Director, Human Resources (or designate) 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.

25.3 RESPONSIBILITY

Director, Human Resources (or designate)

25.4 PROCEDURES

The Director, Human Resources (or designate), in coordination with the Manager, Privacy (or designate), is responsible for investigating 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 Director, Human Resources (or designate) 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 Director, Human Resources (or designate), 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 (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 (or designate).

The Director, Human Resources (or designate) in coordination with the Manager, Privacy (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 the Director, Human Resources (or designate) 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 Director, Human Resources (or designate), 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 of the actions taken. An aggregate summary of such investigations and actions will be included in the annual privacy report to the CEO.

26 CONSOLIDATED LOG OF PRIVACY ISSUES AND RECOMMENDATIONS

26.1 POLICY

OTN maintains a log of privacy issues and recommendations. The Manager, Privacy, the Information Security Manager or designates will monitor and update the log regarding implementation of recommendations. The Manager, Privacy will include a summary of the log as part of the Annual Privacy Report.

26.2 RESPONSIBILITY

Manager, Privacy (or designate)

26.3 PROCEDURES

The Manager, Privacy (or designate) maintains a corporate log of all privacy impact assessments, privacy audits, investigated privacy and security breaches and privacy complaints, together with their related recommendations and implementation status.

The Manager, Privacy (or designate) 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 (or designate) on an annual basis. Please see the Policy and Procedures for Privacy Audits and Monitoring Reviews in section 16 of the OTN Privacy Policy Framework for more details.

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

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

27 CORPORATE PRIVACY RISK REGISTRY

27.1 RESPONSIBILITY

Manager, Privacy (or designate)

27.2 POLICY

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

Risk ID	Risk Description	Risk Level / Rating (high, medium, low)	Status	Notes	Risk Owner

The OTN Privacy Risk Registry is updated monthly by the Manager, Privacy (or designate) and included in the Annual Privacy Report submitted to the Director, Legal and Regulatory Affairs, VP Finance and Administration, and the CEO for approval. In addition, at the prerogative of the Manager, Privacy (or designate), background reports can be appended that take an OTN-wide view of privacy and information security risks and address 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

28 APPENDICES

28.1 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 disclosure, modification or deletion 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.

Confidential and restricted information for purpose of this agreement includes, OTN's personnel, corporate, proprietary information, any personal and personal health information, passwords, hardware security modules, cryptographic keys, held by OTN, as well as information about its relationship to its service providers and other third parties is confidential information.

OTN individuals must be compliant with this and other relevant policies 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 Privacy Audits and Monitoring Reviews 18.88.PP. All information that is maintained, stored, or produced by OTN assets must be consistently protected in accordance with OTN's information & asset classification scheme throughout its life cycle, from its origination to its sanitization to ensure confidentiality, availability and integrity of all information and assets owned and/or managed by OTN (please refer to Information Classification Policy 21.40.P).

28.1.1 Responsibility

Manager, Privacy (or designate) in coordination with Director, Human Resources

28.1.2 Confidentiality Agreement Template

28.1.2.1 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 and regulations or as it may be amended from time to time (PHIPA).
- OTN will only permit access to OTN confidential information for up to one year, upon signature of this agreement. This access may be terminated at any time.

- Managers are responsible for ensuring that access privileges are updated/removed upon job change or termination or their employees or those reporting to them.
- OTN requires that I re-sign a confidentiality agreement on an annual basis within one month of the beginning of OTN's fiscal year (i.e. re-sign by April 30).

28.1.2.2 Purpose of this agreement

This agreement sets out the terms and conditions governing my access, use and disclosure of confidential, personal and restricted 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 upon signature and dating and until OTN's yearly electronic acknowledgement/sign-off.

28.1.2.3 Protection of Confidential Information

I agree to protect confidential information available through OTN by:

- Successfully completing Privacy & Security eTraining on an annual basis where required
- Using it for the purpose it was provided, unless prior written permission is obtained from OTN Manager, Privacy (or designate).
- Access as required in order to carry out my contractual or employment responsibilities.
- Not collect, use, disclose confidential information for any purpose other than the purposes for which the information was collected, used or disclosed or as permitted or required by law.
- 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.
- Protecting PHI from any unauthorized access, use, disclosure including using appropriate security safeguards as identified the Acceptable Use of Information Assets Policy 21.05.P.
- Keeping information that I am responsible for obtaining and entering into OTN systems accurate and up to date.
- Securely disposing of information that I create in accordance with the Retention, Transfer and Destruction of Confidential Information Policy 18.73.PP.
- Protecting and keeping secure computer access codes (for example, passwords).
- Using physical security protection for access devices (for example, keys and badges).
- Refraining from lending my access codes or devices to anyone or attempting to use those of others.
- Accepting legal responsibility for work done under assigned access codes and devices.
- Users must not copy, move, or store confidentiality information onto local hard drives and removable electronic media without explicit approval or business approved standard operations procedure.
- If authorization is granted, taking all necessary steps to protect confidential information against unauthorized use or disclosure.
- Securely returning or destroying confidential information, as requested, in accordance with OTN procedures.

- Notifying immediate supervisor and Manager, Privacy immediately if in receipt of any legal or other demand to disclose confidential information.
- Notifying immediate supervisor and Manager, Privacy immediately of any failure, or potential failure, to protect confidential information in accordance with this agreement.
- 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.
- Using OTN assets in a responsible and accountable way, while maintaining professional decorum at all times.

28.1.2.4 Terms and Termination

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.

28.1.2.5 Signature Block

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

28.2 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: _____

28.3 PRIVACY BREACH CHECKLIST

For more details, please see *Key Steps for Organizations in Responding to Privacy Breaches*[6].
Note: Same steps apply for PHI and/or PI breaches

28.3.1 Step 1: Incident Description

1. What was the date of the incident?
2. When was the incident discovered?
3. How was it discovered?
4. What was the location of the incident? (site name; member/non-member)
5. What was the root cause of the incident?

28.3.2 Step 2: Breach Containment and Preliminary Assessment

1. Have you contained the breach (recovery of information, computer system shut down, locks changed)?
2. 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. Manager, Privacy (or designate), Manager of Security (or designate), communications, risk management, legal)?
3. Have you determined who needs to be made aware of the incident internally and potentially externally at this preliminary stage?
4. Does the breach appear to involve theft or other criminal activity? If yes, have the police been notified?
5. Have you made sure that evidence that may be necessary to investigate the breach has not been destroyed?

28.3.3 Step 3: Evaluate the Risks Associated with the Breach

1. What personal health information (PHI) and/or personal information (PI) was involved?
    - Data elements (name, address, SIN, financial, medical)?
    - Sensitivity?
    - Potential of fraudulent use?
    - What form was it in (e.g., paper records, electronic database, video)?
    - What physical, administrative or technical security measures were in place at the time of the incident (locks, alarm systems, encryption, passwords, policies & procedures, etc.)?
2. What was the root cause and extent of the breach?
    - Is there a risk of ongoing breaches or further exposure of the information?
    - Can the PHI and/or PI 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 PHI and/or PI been recovered?

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

3. 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, members, third-party service providers, partners, vendors, other organizations)?
4. Is there any foreseeable harm from the breach?
5. 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.)?
6. Do you know who has received the information and what is the risk of further access, use or disclosure?
7. What harm to the organization could result from the breach (e.g., loss of trust, loss of assets, financial exposure, legal proceedings, etc.)?
8. 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)?

28.3.4 Step 4: Notification

1. 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.
2. 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 ensuring that the investigation is not compromised?
3. 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 and/or personal health 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).

4. Are there others who should be informed about the breach?
   - Should any privacy commissioner's 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, or other internal or external parties such as third-party contractors, internal business units not previously advised of the privacy breach, and union or other employee bargaining units as applicable.

28.3.5 Step 5: Remediation

1. What remediation activities have taken place?

28.3.6 Step 6: Prevention of Future Breaches

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

28.4 Risk Evaluation Criteria

Table 1.0 Risk Evaluation Criteria

Category	Evaluation Criteria/Examples
Nature of PHI/PI Involved	• Data Elements • Sensitivity • Context • Level of encryption/accessibility • Potential for fraudulent use
Causes and Extent of Incident/Breach	• Determine causes of incident/breach • Determine risk of further exposure of PHI/PI • Determine extent of unauthorized access, collection, use or disclosure of PHI/PI (e.g. number and nature of likely recipients and risk of further access, use or disclosure) • Determine if information is lost or stolen • If information was stolen, was it the target of the theft • Status of information recovery • Steps taken to mitigate harm • Problem is systemic or isolated • Number of individuals impacted • Who is impacted (e.g. staff, contractors, public, HIC, member, etc.)
Risk of Foreseeable Harm	• What are the reasonable expectations of impacted individual? • Who is the recipient of the breached information? • Is there any relationship between data subjects and unauthorized recipients of breached information? • Was unauthorized access or disclosure by/to an unknown party or a party suspected of being involved in criminal activity where there is a potential risk of further misuse? • Is the recipient a trusted, known entity or individual who would be reasonably expected to return the information without disclosing or using it?
Nature of Foreseeable Harm to Affected Individuals/Data Subjects	• Security risk (e.g. physical safety) • Identity theft • Financial loss • Loss of business or employment opportunities • Humiliation, damage to reputation or relationships
Nature of Foreseeable Harm to OTN	• Loss of trust in OTN • Loss of assets • Financial exposure • Legal proceedings (i.e., class action suits)
Nature of Foreseeable Harm to the Public (due to breach or notification of the breach)	• Risk to public health • Risk to public safety

End of Document