Privacy Program

FY 2018/19 Annual Report

September 2019

Care. Connected.

Table of Contents

1. Purpose of the Report

This is OTN's fifth comprehensive Annual Privacy Program Report. The purpose of this report is to describe OTN's Privacy Program and highlight the privacy milestones achieved in the 2018/2019 fiscal year. The Report also includes a summary of key privacy initiatives underway at OTN and trends monitored by the Privacy Team (the Team).

Interdepartmental collaboration is critical to the success of OTN's Privacy Program. The Team relies on support from the following teams, in addition to many others:

- OTN's Senior Leadership Team
- Information Security Office
- Contracts and Legal Team
- Member Services and Adoption Teams
- Technical Operations Team
- Procurement Team
- Marketing & Communications Team
- Project Management Office

2. Contact

Communications regarding this document can be directed to:

Valorie Tutt, Director, Legal and Regulatory Affairs
Ontario Telemedicine Network
438 University Avenue, Suite 200
Toronto, ON, M5G 2K8
t. 416-446-4110 x 4025 / 1-855-654-0888
e. vtutt@otn.ca / privacy@otn.ca

3. Introduction to OTN's Privacy Program

Established in 2006, OTN's Privacy Program has progressed from a one-person office to a virtual privacy and records information management team of certified industry and subject matter experts. The Team offers a suite of privacy and records management services to internal OTN stakeholders, as well as consumers, our partners and their patients. The Team enables OTN to achieve its business goals, while also ensuring compliance, supporting continuous learning and innovation, and strengthening OTN's privacy-focused culture. Over the past fiscal year, the Team demonstrated the strength of its approach through its involvement in several important initiatives, including a primary care model demonstration project and a successful, OTN-initiated meeting with the Office of the Information and Privacy Commissioner of Ontario (IPC).

In 2018-2019, the Team participated in a primary care model demonstration project involving asynchronous messaging, audio, or video calling between physicians and patients. OTN worked in partnership with Local Health Integration Networks (LHINs) and third-party vendors to deliver the project, and the Team was engaged to provide advisory and consulting services on project elements involving patient consent, survey evaluation, and training materials. The Team also led an externally conducted privacy impact assessment (PIA), and contributed to the development of master agreement schedules, data sharing agreements, and requests for proposals. This complex initiative involved multiple stakeholders, vendors, funding partners and relationships. Through early engagement and participation in the project, the Team successfully completed the initiative, which demonstrated clear potential for improved access and care quality, in addition to cost savings for patients. OTN's patient-centered approach to privacy established confidence and trust among project partners, vendors and participating patients.

As part of its commitment to maintaining a trust-based, open and transparent relationship with the IPC, the Team participated in a face-to-face touch point meeting in early 2019. A key objective of the meeting was to provide an update on OTN Privacy Program initiatives undertaken since the last meeting, as well as provide a preview of new initiatives anticipated for the coming year. Topics discussed included OTN's direct-to-consumer services, agile project management methodology, and OTN's evolving role and strategic goals. The meeting was highly productive and highlighted OTN's commitment to privacy.

As Ontario's healthcare system undergoes a period of transformation and structural change, the Team will leverage its considerable expertise and experience to support OTN's strategy, programs and services, while also supporting our partners. In doing so, the Team will continue to rely on a patient and consumer-centered approach to privacy that fosters trust in a world of rapidly evolving technology.

4. Program Objectives

OTN is committed to respecting personal privacy and safeguarding data assets. This includes, but is not limited to, personal information (PI), personal health information (PHI) and anonymized and aggregated data that OTN and its third-party vendors and partners may handle and host on behalf of OTN customers and consumers. OTN responds to rapid changes in technology by continuously adapting, improving, and at times re-designing elements of its Privacy Program. A balanced approach and provincial focus are required to ensure privacy obligations and risks are met and managed on a continuous basis across the organization.

The ever-changing privacy landscape and healthcare system require innovative and adaptable privacy and records information management professionals that are steeped in global privacy laws, healthcare trends, information technology, mobile apps, cloud computing and data analytics. New ways of thinking and new design approaches are also required to ensure privacy is embedded in everything OTN does. The Team is committed to continuous learning and development in support of a privacy program that meets and exceeds these requirements.

5. Governance and Accountability

In a constantly evolving healthcare system and regulatory environment, it is critical that OTN's Privacy Program has a robust foundation from which to pivot and adapt. To that end, OTN's Privacy Program has an established governance and accountability structure as outlined in the table below.

Roles	Responsibility
Board of Directors	Responsible for the overall effective governance of OTN affairs. Holds fiduciary accountability for OTN and is responsible for the organization's compliance with applicable laws, including privacy legislation.
Planning and Priorities Committee of the Board	A committee of the Board that provides leadership and governance oversight for OTN's strategic planning and risk management activities. The committee reviews OTN's risks and ensures appropriate risk management activities are undertaken, including risks related to privacy and information security.
Chief Executive Officer (CEO)	Has been delegated authority to operate OTN on a day-to-day basis and implement policies and practices, including those related to privacy, information and risk management.
Senior Leadership Team (SLT)	Led by the CEO, Manages the day-to-day business of OTN, the SLT approves privacy and information security policies, and provides senior management with direction on major privacy and information security issues.
Vice President Finance and Administration	Executive sponsor for the Privacy Program and oversees the privacy function at OTN.
Chief Operating Officer (COO)	Is the senior executive accountable for overseeing the information security function at OTN.
Executive Lead, Platform, Products & Integration	Executive Lead at OTN responsible for enterprise architecture, platform redesign and implementation.
Director, Dev Ops and Infrastructure (includes information security operations	Accountable for the information security function at OTN and for the security of OTN information systems in collaboration with Privacy Team.
Manager, Information Security	Responsible for managing information security activities at OTN. Accountable for reviewing, auditing and providing advice on the Information Security Program, in alignment with industry standards, to maintain the confidentiality, integrity, and availability of all OTN information systems.

Roles	***Responsibility***
Information Security Specialist	Responsible for managing the security of OTN information systems, investigating security incidents, reviewing audit logs, and for conducting Threat and Risk Assessments (TRA(s)).
Director, Legal and Regulatory Affairs	Has administrative responsibility for the Manager, Privacy, and provides oversight and guidance to the Manager. Reviews and approves privacy initiatives in support of new lines of OTN business.
Manager, Privacy	Oversees and manages all aspects of OTN's Privacy Program and provides privacy, policy and compliance leadership for a variety of stakeholders both internal and external to OTN.
Privacy Specialist	Responsible for providing privacy assurance services to OTN functional areas and projects, conducting privacy impact assessments (PIA(s)), investigating privacy incidents, reviewing policies, and other related responsibilities.
Records & Policy Management Specialist	Responsible for providing subject matter expertise on records management processes to ensure OTN's compliance with legal, business, archival and audit requirements for the tracking, storage, retention and destruction of confidential and official records. Tracks, formats and ensures accuracy of policies in compliance with OTN branding standards. Co-ordinate the publishing of policies and effectively communicates updates to policy owners.
Privacy & Security Lateral Team (PSLT)	Chaired by Vice President, Finance and Administration. This cross-functional team provides advice and guidance with respect to privacy and security initiatives being contemplated and undertaken by OTN's Privacy and Security Programs and directs the requirement for broader organizational consultation when needed.

6. OTN's Privacy Operational Plan

The Team identifies key operational objectives on an annual basis and incorporates these into its Privacy Operational Plan. The Operational Plan is aligned to key organizational and provincial strategic priorities. It also informs individual team plans, as directed by the Ministry of Health (the Ministry) through public funding sources.

6.1. Operational Plan 2018/2019: A Year in Review

Highlighted below is a key initiative the Team led in 2018/2019, in alignment with that year's Privacy Operational Plan.

6.1.1. Direct-to-Consumer Services and Integrated Privacy Policy Framework

OTN has successfully introduced a series of important consumer-based health services to Ontarians. Some of the services, like Big White Wall (BWW,) are OTN-managed, while others, like Bounce Back or CanImmunize, are delivered by third parties. As part of these services, OTN collects, uses and discloses PI to connect consumers to OTN services and/or external services.

OTN recognizes its responsibility to protect consumer information that falls outside the scope of the *Personal Health Information Protection Act, 2004* (PHIPA), as well as its obligation to provide notice of information practices related to consumer-facing services. As such, OTN tailored its Privacy Program to include the management of consumer PI through new and revised policies, practices and notices.

OTN followed the Office of the Privacy Commissioner of Canada's guidelines, and leveraged the Fair Information Principles (FIPs) to develop its direct-to-consumer information practices and create an Integrated Privacy Policy Framework. The Integrated Privacy Policy Framework synthesizes OTN's policies and practices with respect to its traditional telemedicine services and the new direct-to-consumer services.

6.2. Operational Plan 2019/2020: Innovation Through Service That's One Step Ahead

OTN's 2019/2020 Privacy Operational Plan is designed to support and enable OTN's new multi-year strategy and transformation initiatives, in alignment with the provincial government mandate. Key initiatives are summarized below.

6.2.1. Ontario's Healthcare Transformation

In 2019, the Ministry introduced plans for a provincial integrated patient care model under the newly created Ontario Health Agency. OTN has undertaken extensive planning and developed strategies to support this new super agency. *The People's Health Care Act, 2019*, gives the Minister the power to transfer assets, liabilities, rights, obligations and employees of certain organizations to the Agency, a health service provider or an integrated care delivery system. This new structure will result in new roles and authorities under PHIPA regarding the permitted collection, use and disclosure of PHI[1]. Noted below are key excerpts directly from the Information and Privacy Commissioner of Ontario's comments on *The People's Health Care Act,* in terms of recommended changes to PHIPA and its Regulation 329/04[2]:

- *Make appropriate designations under PHIPA*: An organization's designation under PHIPA determines the PHI it can collect, use and disclose and its obligations with respect to that information. Making appropriate designations under PHIPA will give the Agency the legal authority for these collections, uses and disclosures, while ensuring that the privacy and access to information rights of Ontarians are protected. Designation under PHIPA will also give the Information and Privacy Commissioner oversight of the Agency's information practices.
- *Require that PHI collected, used, or disclosed for different purposes be retained separately:* PHI collected, used or disclosed by the Agency for one purpose must be kept administratively and logically separate from information collected, used or disclosed for other purposes, unless a comprehensive framework with appropriate safeguards and oversight is put in place.
- *Designate Integrated Care Delivery Systems as Health Information Custodians:* In order for integrated care delivery systems to be able to effectively integrate services provided by health service providers who are all health information custodians (HIC(s)) under PHIPA, the integrated care delivery systems must themselves be subject to the same legislative framework as health service providers.

The Team is actively monitoring for changes to the legislation. The Team is also working closely with the Data Governance and Business Intelligence Teams to anticipate and plan for changes to our information practices that may be required

[1] Brian Beamish (2019), "Comments of the Information and Privacy Commissioner of Ontario on Bill 74" [Online]. Available: https://www.ipc.on.ca/wp-content/uploads/2019/04/2019-03-bill-74.pdf [2019, July].

[2] Ibid.

when these legislative changes are enacted. With approval from the Enterprise Business Office Steering Committee, a data governance and regulatory framework tailored specifically for OTN will be delivered by external consultants. The completion of this framework is anticipated for Q3 2019/2020.

6.2.2. Partner Video Project

Following the success of a proof of concept limited enrollment pilot completed last fiscal year, OTN is moving forward with a project to test how alternative video solutions can be introduced and scaled in Ontario. The Partner Video Project enables health care organizations and affiliated providers to use the videoconferencing services of their choice on a proof of concept basis. The Team has provided significant input into the creation of "organizational readiness criteria" to help prepare and assess OTN's partners' readiness to safely, securely and successfully launch and use their video solution of choice. The goal is to ensure that privacy and information security are built into organizations' plans and governance frameworks, and to support OTN's partners in meeting privacy obligations and legislative requirements, along with bandwidth and implementation considerations. OTN will also provide support in terms of videoconferencing etiquette and best practices.

6.2.3. Bring Your Own Device

OTN increasingly offers services directly to consumers and patients. One such service, the Telehomecare program, brings chronic disease management and progressive lung disease intensive coaching to patients in their own homes. OTN is expanding this service by enabling patients to use their own devices to manage their own care. OTN will roll-out a "bring your own device" initiative as part of this provincial program. The Team will be involved in assessing the actual or potential effects that this service will have on the privacy of patients and will provide recommendations to mitigate any identified risks. It is expected that this service will be available in Q3 of 2019/2020.

7. OTN's Privacy Program: Key Components

7.1. Privacy Policies and Procedures

OTN has established a comprehensive suite of privacy policies, as well as a policy management framework, to guide its Privacy Program and culture. The policy management framework triggers reminders for expiry dates and facilitates the timely review of policy documents. This ensures that OTN's privacy policies are kept current and up-to-date. A number of new consumer-facing policies have been created and will be included in OTN's Integrated Privacy Policy Framework (see section 6.1.1 of this report). These new policies deliver enhanced transparency and accountability with respect to OTN's management of PI.

7.2. Privacy Consultation, Assurance and Risk Management Services

The Privacy Team provides assurance and advisory services to OTN's Project Management Office (PMO), Enterprise Business Support Office, and other OTN business functions and programs. Privacy assurance and advisory services are also provided to external stakeholders and Members as required. Additionally, the Team is involved in OTN's Project Gating process and Project Management Lifecycle methodology to pre-emptively identify and mitigate risks.

The Team's engagement during early project phases ensures that privacy considerations and safeguards are embedded into each step of a project's design and delivery. This approach also drives innovation, reduces costs and prevents last minute re-work and project delays. Furthermore, it instills trust and confidence that OTN services and programs will not only improve access to care, but also provide a positive privacy experience for customers, patients and other key stakeholders.

The Team provides the following consultation, assurance and risk management services:

- Privacy consultation with the Senior Leadership Team, project teams, vendors and partners.
- Privacy Threshold Assessments.
- PIAs and mitigation plans.
- Privacy and Security Architecture design documents.
- Privacy Statement of Risk.

- Subject-matter expertise (SME) contributions to systems architecture, solution design and interfaces, change management and business requirements documents.
- SME contributions to Request for Information, Request for Proposal and Statement of Work documents and processes.
- Language for and review of agreements and other legal artefacts, such as Master Service Agreements, Terms of Service, Data Sharing Agreements, notices, privacy statements.
- SME contributions to privacy communication and training materials.
- Development of and updates to privacy, security and other relevant policies and procedures.
- Consultation with the Information and Privacy Commissioner, legal counsel and other external partners as required.

7.2.1. Initiatives Led or Supported by the Privacy Team in 2018-2019

Privacy Assurance Service	Project	Total 2017/ 2018	Total 2018/ 2019
PIAs led by external consultants with oversight from OTN's privacy specialists	***2018/2019*** • Secure Messaging PoC (iOS) • Secure Messaging PoC (Delta) Android & OTNhub • eConsult • EAPC Novari phase I • EAPC Novari phase II & III (Delta) • EAPC TRC Research phase I • EAPC TRC Research phase II & III (Delta) •• BWW Provincial Program	8	8
Internal Privacy Risk Review or Privacy and Security Architectures (PSA(s)) conducted by OTN privacy specialist	***2018/2019*** • Telehomecare- Vivify_Diagnostic Report API HRM and OTN eFax • Telehomecare- Vivify_BYOD	2	2
Other Privacy Assurance Services	• Consultation by design requirements • Development of initiative and project artefacts	43	49

	• Consulting Agreements • Service Agreements • Vendor Service Agreements • Statements of Work under established Master Service Agreements • Updates to OTNhub Terms of Service and User Agreement • Data Sharing Agreements • Pilots and Proof of Concepts (Terms of Service, User Agreements, End User License Agreement, and memorandums of understanding) • API Terms		

*Privacy and security deliverables for Canada Health Infoway-funded projects include PIAs, TRAs and PSAs.

7.3. Monitoring and Compliance

OTN has monitoring and compliance policies, practices and tools which include, but are not limited to, the following;

- Incident reporting and investigation tools
- Risk identification and mitigation strategies (such as PIAs, TRAs and PSAs)
- Privacy scorecard
- Privacy risk register
- Compliance and monitoring policy and reporting tool
- Mandatory staff orientation and training
- Policy/guideline review processes
- Inquiry tracking & trending

7.4. Privacy Incident Management

OTN has implemented a Privacy Breach Management Policy and Procedure. The following situations trigger a privacy investigation and escalation process in accordance with the Policy:

- There has been an unauthorized access, collection, use, retention, disclosure or disposal of PHI, personal information (PI) or confidential information.
- There is a suspected unauthorized access, collection, use, retention, disclosure or disposal of PHI, PI or confidential information.
- An unauthorized person has accessed PHI, PI or confidential information either accidentally or intentionally.

- A situation occurs which might cause any of the above three scenarios to occur in the future if action is not taken.

Incident reporting is a shared responsibility between OTN, its members and users. Responsibility for investigating incidents, and documenting ivestigation findings, is triaged by the Manager, Privacy, to a member of the Team as appropriate. OTN has a detailed escalation and notification process based on incident severity. OTN reports all medium and high-severity breaches to the Ministry through its corporate scorecard.

OTN's role under PHIPA differs by OTN service (see the Appendix for a complete list of OTN's roles). In the context of OTN's virtual care services, which involve health care providers and patient PHI, OTN is not a HIC. As such, OTN does not directly notify patients of privacy breaches involving their PHI. Information is passed on to the appropriate HIC(s), who is then responsible for notifying affected patients in accordance with its own incident management procedures. In the event of a privacy breach involving PI in OTN's direct-to-consumer services, OTN will notify impacted consumers where there is a real risk of significant harm. Where appropriate, opportunities for improvement are identified and recommended to applicable stakeholders.

During a privacy breach investigation, the assigned OTN Privacy Specialist develops a plan to mitigate any identified risks and ensures that the plan is implemented. Once immediate steps have been taken to mitigate risks associated with the breach, OTN completes a root cause investigation. If necessary, this includes a security audit of physical, administrative and technical controls. Based on the results of this evaluation, the Team will assist the responsible unit(s) to implement adequate long-term safeguards that protect against further breaches. Policies will be reviewed and updated to reflect the lessons learned from the investigation. The resulting plan will also include audit recommendations where appropriate.

Following a privacy investigation, the Team works with members, users and internal subject matter experts to identify improvement opportunities and drive the implementation of privacy best practices to prevent similar breaches in the future.

The Team tracks all privacy investigations, including near misses and confirmed non-breaches. Breaches related to both PHI and PI are tracked and recorded. Key metrics related to privacy investigations are reported on the privacy scorecard (see section

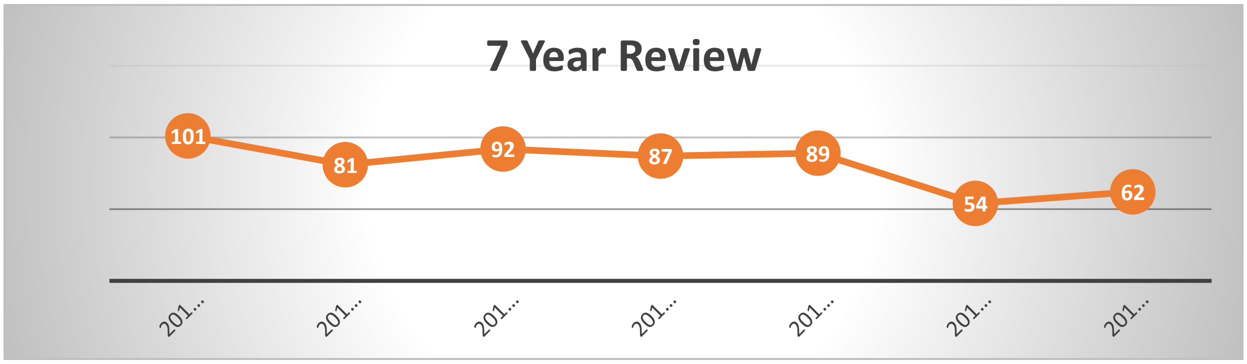
7.7). Incident tracking allows the Team to identify trends and improvement opportunities for both OTN employees and members.

7.4.1. Privacy Investigations and Breaches in 2018-2019

In 2018/2019, the Team saw a slight increase in the total number of reported privacy incidents, from 54 the previous year to 62 (see the table below). The number of incidents identified as breaches also increased from 17 in 2017/2018 to 25 in 2018/2019. It is likely that this increase is related to the first full year of mandatory privacy breach reporting under PHIPA. Additionally, on November 1, 2018, new provisions in the *Personal Information Protection and Electronic Documents Act* (PIPEDA) related to breaches of security safeguards came into force. Finally, OTN's expanded work with third-party vendors has introduced new privacy challenges. OTN continues to work diligently with third-party vendors to support improvements to its privacy practices and breach management protocols.

Privacy Investigations	***2012-2013***	***2013-2014***	***2014-2015***	***2015-2016***	***2016-2017***	***2017-2018***	***2018-2019***
Total # of Incidents Investigated	101	81	92	87	89	54	62
Total # of breaches	50	64	40	25	28	17	26
Breaches Due to: *OTN Action*	*33*	*32*	*19*	*12*	*13*	*10*	*6*
Member Action	*12*	*30*	*19*	*12*	*13*	*7*	*11*
OTN and Member Action	*5*	*2*	*2*	*1*	*2*	*0*	*0*
Vendor/Partner	*n/a*	*n/a*	*n/a*	*n/a*	*n/a*	*n/a*	*9*
Breach Severity							
Breaches High Severity	0	0	0	0	0	1	0
Breaches Medium Severity	4	0	1	0	1	0	4*
Breaches Low Severity	46	64	39	25	27	16	22

*4 privacy breaches related to the Enhanced Access to Primary Care Proof-of-Concept. PHI was disclosed by OTN's third party vendor delivering the technical platform/solution, to unauthorized healthcare providers as a result of human error.

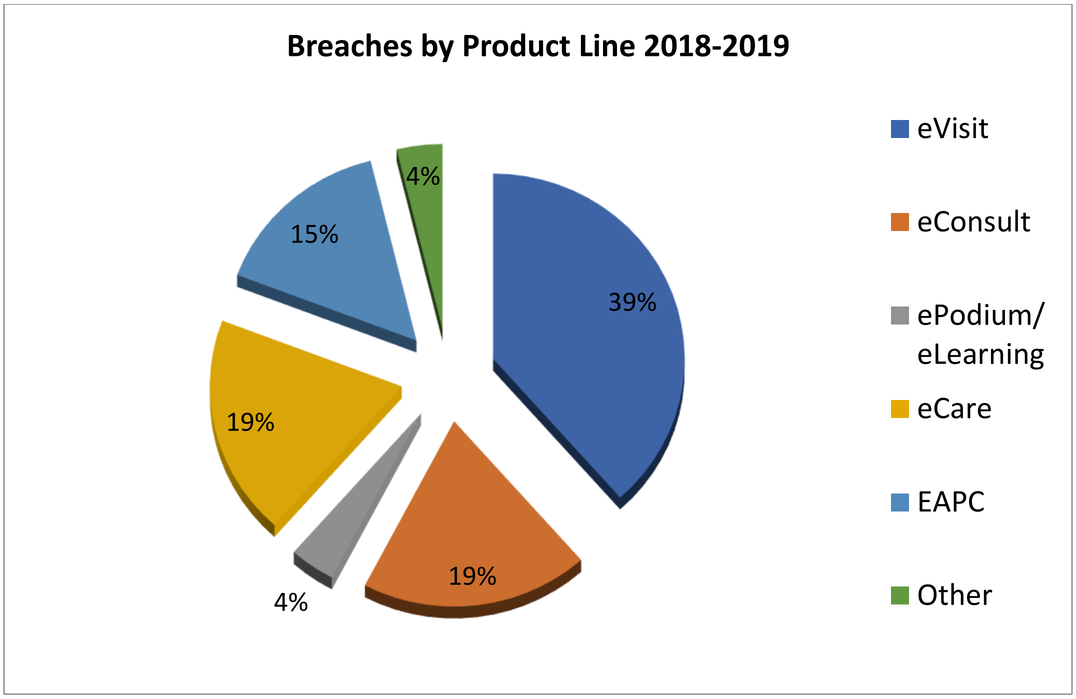


7.4.2. Privacy Breaches by Product/Service

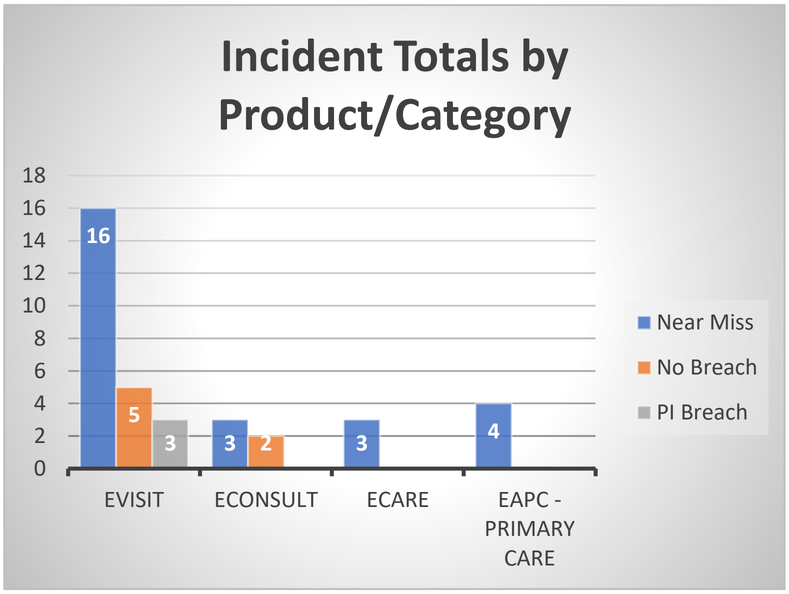
OTN's videoconferencing solutions are used to provide over 1.145M virtual visits annually. Behaviours related to videoconferencing and scheduling remain the primary source of privacy breaches reported to OTN.

Breaches by Product/Service	***2012-2013***	***2013-2014***	***2014-2015***	***2015-2016***	***2016-2017***	***2017-2018***	***2018-2019***
Room-based videoconferencing	41	52	25	16	8	5	2
OTNhub	n/a	n/a	n/a	n/a	2	1	0
eConsult/Store Forward (Telederm)	8	5	3	2	2	2	5
Personal Videoconferencing	0	3	4	1	2	0	3
Telemedicine Service Manager/Ncompass	0	0	3	4	10	6	2
Telehomecare	0	0	0	0	2	1	5
Teleophthalmology	0	1	2	0	0	0	0
Webcasting	1	3	3	2	1	0	3
Emergency Services	0	0	0	0	0	0	0
Learning Center	0	0	0	0	0	0	0
EAPC – Primary Care	n/a	n/a	n/a	n/a	n/a	n/a	4
Other	n/a	n/a	n/a	n/a	1	2	2*
Total	***50***	***64***	***40***	***25***	***28***	***17***	***26***

*2 unrelated to OTN services – misdirected fax sent to OTN meant for another organization and suspected internal office access and printer authentication compromised.



As mentioned above, OTN continues to experience a high number of incidents related to videoconferencing behaviours, relative to other product lines. In 2018/2019 the Team investigated a total of 24 incidents related to videoconferencing, including 16 “near misses”, 5 investigations which were classified as “no breach” and 3 “personal Information (PI) breaches”.



The “near miss”, “no breach” and “PI breach” incident classifications are defined below:

Near Miss: A situation has occurred that could have resulted in non-compliance with PHIPA and /or its Regulation, but no patient PHI was involved. Near misses provide opportunities to identify and mitigate risks in our systems and processes before they impact privacy and patient care.

No Breach or Non-Issue: A situation was reported and investigated but was not found to be a privacy breach or incident.

PI Breach (low severity): A contravention of OTN's privacy policies, procedures or practices occurred but there was little or no impact to the organization or affected individuals (e.g., a laptop containing confidential information is stolen from an employee's vehicle, however the laptop was encrypted).

7.5. Privacy Training and Awareness

7.5.1. For OTN Employees

OTN provides comprehensive privacy training for its employees, contractors, and third-party providers. OTN's privacy training covers a range of topics, including privacy and information security principles, policies, procedures, best practices and guidelines. OTN delivers the training and awareness in the following ways:

1. All OTN employees complete privacy training using OTN's privacy online learning e-module. Privacy training is mandatory and is to be completed by all staff within 4 weeks of their start date. Completion of an annual refresher is also required. The privacy module consists of numerous privacy lessons, including:

    - Introduction to Canadian privacy legislation
    - OTN's responsibilities under the law
    - Privacy at OTN
    - Identifying PHI and PI
    - Protecting confidential information
    - OTN's Privacy Policy Framework
    - Privacy incident management
    - Privacy best practices
    - Mandatory breach reporting
    - OTN's direct-to-consumer services
    - Canadian Anti-Spam Legislation (CASL)
    - How and when to contact the OTN Privacy Office

2. All OTN employees are required to sign a Confidentiality Agreement at the start of their employment and annually thereafter.

3. All OTN contractors and third parties agree to the terms of the Confidentiality Agreement and appropriate privacy provisions.

4. All employees are introduced to their privacy obligations during OTN's new hire employee orientation.
5. Member Services and PMO staff complete enhanced privacy training.
6. From time to time, OTN executes education and poster campaigns and other privacy awareness activities. These activities may include blogs or articles in the "OTN Update" newsletter.

7.5.2. For OTN Customers and Members

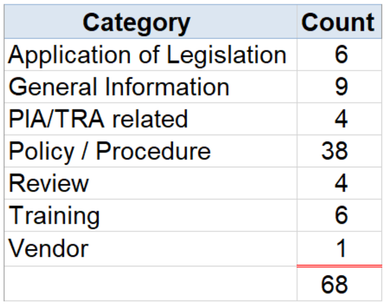
The Team works collaboratively with other OTN departments to activley respond to the learning and education needs of members and customers. Training sessions are offered to both new and existing members and customers through various modalities. OTN has also created a Privacy Centre on www.otn.ca. The purpose of the Privacy Centre is to provide Ontarians and health care providers with information, tools and best practices as they relate to virtual healthcare.

Ongoing privacy training for members and consumers is critical to ensuring the privacy and security of PI and PHI in a complex and dynamic virtual healthcare environment. To that end, the Team continuously refreshes and updates its privacy awareness and training artefacts and develops member and consumer-facing awareness materials.

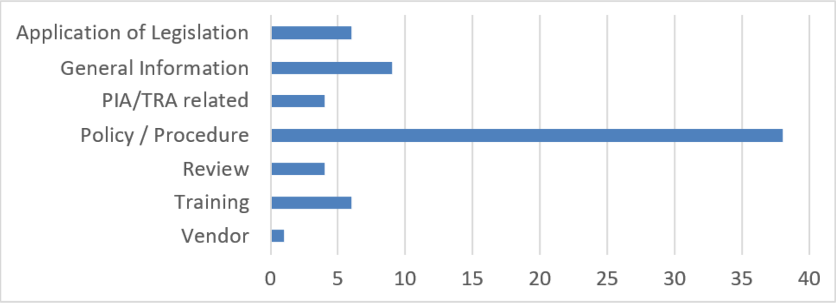
7.6. Privacy Complaints and Inquiries

OTN has a Privacy Complaints and Inquiries Policy. This policy applies to all OTN employees, as well as 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. Privacy inquiries may relate to OTN's privacy policies, procedures and practices as set out in OTN's Integrated Privacy Policy Framework, or compliance with PHIPA and its Regulation 329/04. Information regarding the privacy inquiry process is publicly available on OTN's website at www.otn.ca.

When a privacy inquiry is received, a member of the Team enters the details of the inquiry into a privacy inquiries log. A determination is made regarding the nature of the inquiry and the appropriate response. The following table outlines the number and type of privacy complaints and inquiries received by OTN for fiscal year 2018/19:



Category	Count
Application of Legislation	6
General Information	9
PIA/TRA related	4
Policy / Procedure	38
Review	4
Training	6
Vendor	1
	68



7.7. Privacy Scorecard: Metrics and Reporting

OTN documents a number of privacy metrics (such as number of incidents investigated, training completed by OTN staff, number of closed risks) via its privacy scorecard. These metrics are tracked and monitored for trends over time. The scorecard is reported in its entirety to OTN's PSLT. Certain key indicators are also reported to the Senior Leadership Team, as well as to the Board and Ministry.

The Team also tracks metrics related to project activity. These metrics inform program and project leads of key privacy indicators and improvement opportunities for their program.

7.8. Privacy Impact Assessments and the Privacy Risk Register

A PIA is a risk identification tool that allows OTN, in its various roles under PHIPA[3], to assess a technology, program or information system's privacy risks and its compliance with provincial and federal legislative requirements. PIAs allow OTN to communicate with confidence that privacy requirements have been, or are being, met and identify those risks where mitigation is in progress. PIAs also build trust with members, users, patients and consumers. OTN publishes PIA summaries in its "Privacy Toolkit" on www.otn.ca and shares them with members and users, in accordance with its obligations under PHIPA.

A PIA is meant to be used and expanded throughout an initiative's development and implementation. PIAs are refreshed over time to continuously identify and address risks that have the potential to impact the confidentiality, integrity and accessibility of PI and/or PHI collected, used, and/or disclosed by OTN and its partners.

A PIA provides recommendations for risk mitigation and an action plan. A critical element of OTN's PIA process is the implementation of recommendations detailed in

[3] A complete description of OTN's roles under PHIPA for each OTN service is provided in the Appendix

the assessment, and the development of a Services and Safeguards document. OTN has adopted a risk tolerance level of low. This means that low and very low risks may not be immediately actioned, but will be monitored to ensure that they stay within tolerable levels. All high and medium risks are addressed with mitigation plans which must be documented and approved by the business prior to the launch of the initiative.

The Privacy Program has established a privacy risk register to document, track and monitor risks and recommendations identified in PIAs. These risks are reported to the PSLT as part of the privacy scorecard metrics. Additionally, OTN conducts Threat Risk Assessments (TRAs) under the leadership of the Information Security Team. The Privacy and Information Security Teams work together to implement mitigation strategies for all identified vulnerabilities and risks.

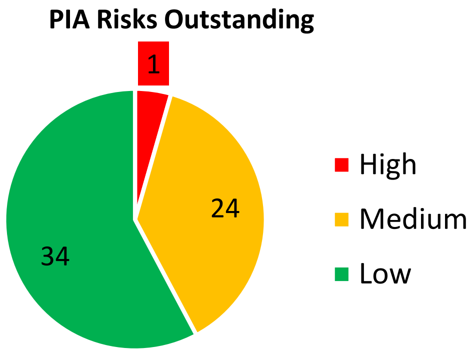
7.8.1. 2018-2019 PIA Findings

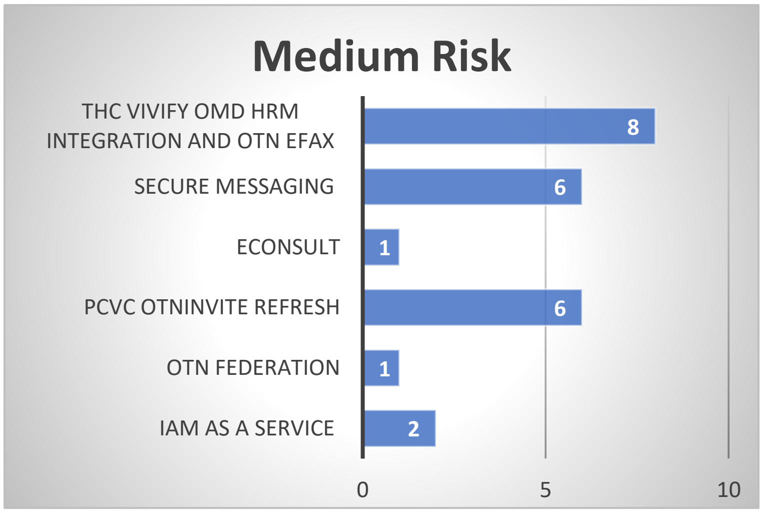
In 2018/2019, eight PIAs were conducted by external vendors of record with oversight by OTN Privacy Specialists, and two internal privacy reviews were completed by an OTN Privacy Specialist directly. 51 risks were carried over from the previous fiscal year and, over the course of 2018/2019, 34 new risks (11 high risks, and 23 medium risks) were added to the privacy risk register (see screenshot of PIA risk register below).

By the end of 2018/2019, 57 risks were closed. The Team continues to track and monitor one high risk (see the table under section 7.8.2 below) and 17 medium outstanding risks. OTN management has accepted these risks, as interim mitigation measures have been implemented and plans developed for complete mitigation in the future. OTN's policy and practice is to mitigate all medium and high risks prior to launching a new initiative, or prior to a new release or upgrade for an existing product or service. However, due to competing priorities, and with approval by the Senior Leadership Team, some risks are mitigated over a longer duration.

7.8.2. Risk Register Snapshot

Source	***High Risk***	***Recommendation***	***Estimated Closed Date***
THC Vivify OMD HRM Integration and OTN eFax #3	OTN is not able to fully comply with this requirement today. A summary has been publicly posted. However; it should be updated to reflect enhanced functionality.	Update current PIA Summary to reflect integration with OntarioMD HRM and OTN RightFax.	Q2 2019-2020 (Project launch planned for July)





7.9. Records Management

The OTN Privacy Program maintains a Retention and Sanitization Schedule for all OTN records, including sensitive records. The Schedule ensures that retention, archiving and destruction practices are consistent with industry standards.

A robust records management program allows an organization to ensure compliance and proactively and progressively manage all data, media and information. OTN's records management mandate is to ensure:

1. Security
2. Access to records

3. Secure document destruction
4. Accountability
5. Accuracy

OTN's best business practices with respect to records management are based on:

1. Federal and provincial legislative requirements
2. The Ministry mandates
3. Corporate policies and procedures
4. OTN's business requirements.

8. Policy Office

The Team provides oversight, support and tracking for all OTN policy documents. The mandate of the Policy Office is to create a robust policy governance and management framework, with processes and practices that align with and support strategic directions, core principles and regulatory and governance requirements to protect OTN and its stakeholders, and to guide change where necessary.

In 2018/2019, OTN had 167 policy documents in place with 68% (114) current and up-to-date. Of these, 6 documents were archived. Additionally, 21 new policy documents are being authored. Automated notifications prompt policy owners to review and update policy content in accordance with revision schedules. Due to competing priorities, reviewing policy documents according to defined review dates has been a challenge. OTN management has established plans to address all areas of non-compliance in 2019/2020.

Types of Document	*Total # of Documents*	*Documents Archived in 2018*	*Under Review by Owner as of March 2019*	*New Documents Under Development*
Policy	55	1	22	12
Policy & Procedure	64	1	23	1
Guideline	18	3	4	1
Standard	5	0	0	0
Form	25	1	4	7
Total	167	6	53	21

9. CASL

CASL took effect in 2014. In response to the legislation, OTN implemented a compliance program to ensure its email marketing programs and subscription newsletters comply with the consent, formalities and unsubscribe requirements under CASL. As part of its CASL Compliance Program, OTN has adopted an express consent model (the gold standard). Supporting business processes have also been implemented, along with tools procured through Broader Public Sector (BPS) procurement directives.

OTN has embedded CASL consent mechanisms in its online onboarding process for members and users. When a member or user signs-up for an OTNhub account or registers to become a member, they are asked for consent to receive marketing emails and newsletters during its/their first interaction with OTN. Similarly, if a visitor to OTN's website signs-up to receive newsletters, the visitor's consent is requested. Additionally, mechanisms to manage subscription preferences at any time post-sign-up are provided.

9.1. CASL Enforcement

The importance of OTN's CASL Compliance Program is underscored by the volume of CASL violations reported in Canada since the legislation took effect. Between April 1 and September 30, 2018, Canadians reported over 5,000 CASL violations per week to the Spam Reporting Centre[4]. The violation reports indicated "emails sent without consent" as the primary complaint[5]. Additionally, in July 2018, the Canadian Radio-television and Telecommunications Commission (CRTC) took enforcement action to combat the installation of malicious software through online ads. As part of this enforcement action, $250,000 in administrative monetary penalties (AMPs) were levied against two separate companies[6].

The volume of reported violations, and the enforcement action described above, highlight the severity of fines for CASL non-compliance and the need for a robust compliance program. Furthermore, the private right of action under CASL remains on-

[4] Innovation, Science and Economic Development Canada (2019), "Canada's Anti-Spam Legislation" [Online]. Available: https://www.fightspam.gc.ca/eic/site/030.nsf/eng/home [2019, July].

[5] Ibid.

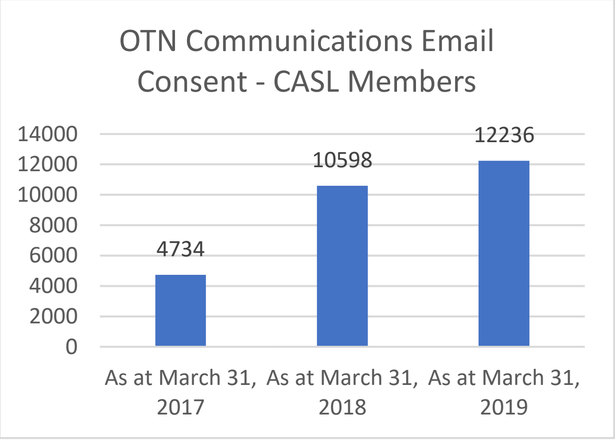
[6] Canadian Radio-television and Telecommunications Commission (2018), "CRTC Issues $250,000 in Penalties to Combat Malicious Online Advertising" [Online]. Available: https://www.canada.ca/en/radio-television-telecommunications/news/2018/07/crtc-issues-250000-in-penalties-to-combat-malicious-online-advertising.html [2019, July].

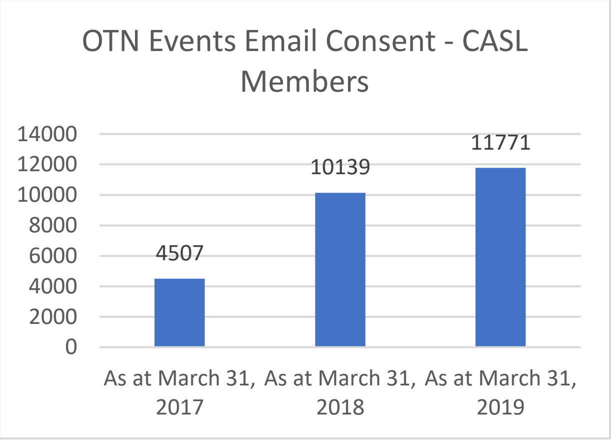
hold. When it takes effect, the possibility of legal proceedings by individuals and organizations seeking compensatory damages will significantly increase the risks associated with CASL non-compliance.

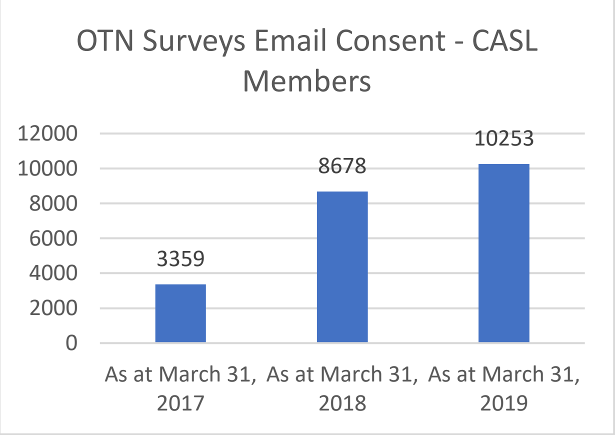
9.2. OTN's CASL Compliance Program: A Success Story

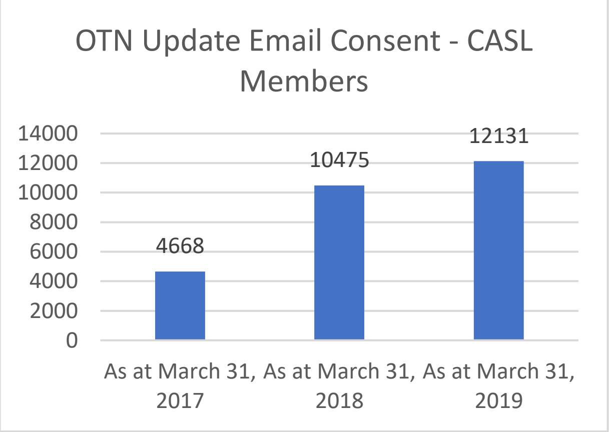
OTN regularly reviews and updates its CASL Compliance Program, which includes staff education, consent monitoring, policy adherence and other compliance activities. A commitment to quality documentation and excellent record-keeping builds and maintains trust with members, users and the public, and ensures that OTN can clearly demonstrate its compliance efforts.

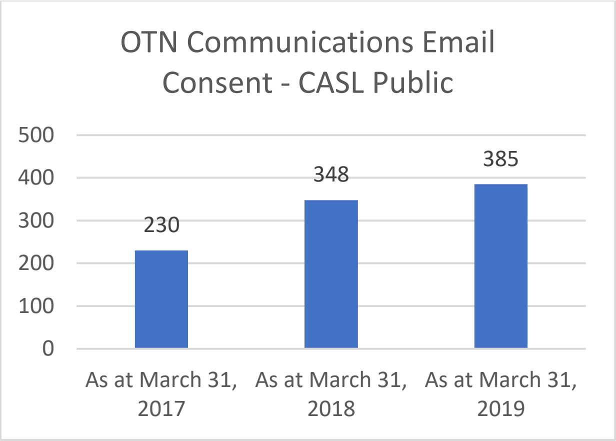
OTN's CASL Compliance Program and implementation of an express consent model correlate with a substantial rise in OTN subscriptions, as illustrated in the charts below. While several factors likely contribute to subscription growth, the mechanisms implemented by OTN to obtain express consent have not discouraged subscriptions.

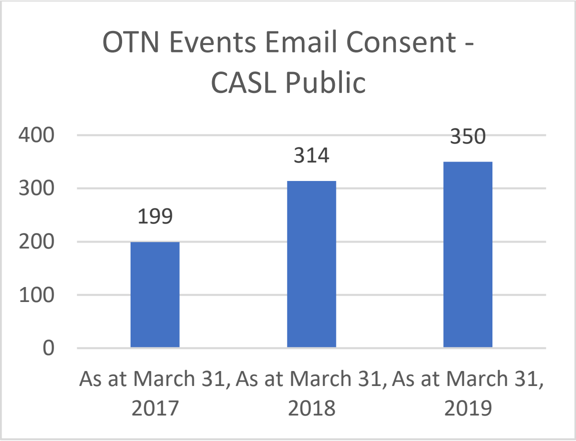

OTN Communications Email Consent - CASL Members


OTN Events Email Consent - CASL Members


OTN Surveys Email Consent - CASL Members


OTN Update Email Consent - CASL Members





OTN's well-established CASL Compliance Program builds trust and helps ensure the protection and appropriate use of member, user and consumer information.

10. Trends Shaping and Informing OTN

The Team strives to create and sustain an environment that breeds continuous learning and innovation. The Team is forward-focused and monitors provincial, federal and global privacy trends, allowing OTN to readily adapt to changes and integrate evolving best practices into its Privacy Program. The following are key trends shaping OTN and the larger privacy landscape:

- Cloud migration
- Third-party vendor management
- Internal transition to digital collaboration tools (MS Teams and SharePoint)
- Direct-to-consumer services (see section 6.1.1)
- Phishing and social engineering

10.1. Cloud Migration

Following the completion of a PIA and TRA, OTN successfully transitioned some of its operations to a cloud environment and cloud applications hosted by a third-party vendor. OTN is also in the infancy stages of planning the full migration of OTNhub services to the cloud. This initiative will enable improved web application security, a reduction in data centre footprint, and increased availability and efficiency of service offerings. The initiative will also improve continuous integration pipelines, resulting in faster deployment to production.

The Team has engaged in early collaborative discussions around the migration of OTNhub services to the cloud. This has allowed the Team to consult with key stakeholders with the aim of embedding privacy protections in the project design. A comprehensive external PIA and TRA will be conducted prior to the migration of any OTNhub services to the cloud. These assessments will ensure that OTN has appropriate privacy and security controls in place.

10.2. Third-Party Vendor Management

OTN continues to expand its work with third parties and technology vendors. In doing so, OTN hopes to improve access to care, making it faster and more convenient for patients and healthcare providers. OTN executes agreements with all third parties, ensuring roles, responsibilities, and obligations are set out in advance. OTN third-party agreements also include a privacy schedule which clearly identifies key accountabilities, expectations and required privacy protection measures.

The Team has implemented clear performance and verification policies to manage any privacy and security risks that arise from relationships with third-party service providers. OTN works closely with these providers to document incident management policies and procedures, conduct testing and provide training. Frequent engagement with third-party providers ensures a collaborative approach to managing and remediating risks and implementing strong privacy and security controls.

10.3. Internal Transition to Digital Collaboration Tools (MS Teams and SharePoint)

As a publicly funded organization, OTN is bound by the BPS Procurement Directive. The purpose of the BPS Procurement Directive is to ensure publicly funded goods and services are acquired through a process that is open, fair and transparent. Last year, OTN transitioned to SharePoint Online and Microsoft (MS) Teams for virtual meetings. OTN adhered to the BPS Procurement Directive in its acquisition of these new tools. MS Teams was introduced to support communication and collaboration amongst a dispersed workforce. OTN's adoption of MS Teams was also intended to reduce information silos and redundancies in data and work effort by automating business processes and centralizing information. As a result, staff productivity has improved, and integrated tools and processes have resulted in enhanced support for priority and operational projects.

10.4. Phishing and Social Engineering: Attacks Increasingly Directed at Executives

OTN's Privacy and Security Teams monitor new, emerging and established threats and trends in data security. OTN is committed to sharing knowledge with our partners in the healthcare system to support the effective protection and safeguarding of member, patient and consumer information.

In 2018/2019, OTN experienced social engineering (phishing) incidents specifically targeting senior management. New data indicates that such attacks are becoming more common. Results of the 2019 Verizon Data Breach Investigations Report indicate that senior executives are increasingly targeted in social engineering attacks: "C-level executives are 12 times more likely to be the target of security incidents and 9 times more likely to be the target of data breaches than in last year's report while the growth of financial social engineering attacks targeting these business executives rose from single digits to dozens in this year's report."[7] Senior executives are often targeted because of their authority to approve financial transactions. Additionally, the large volume of email and other communications requiring their attention makes it easier for sophisticated phishing emails to "slip through".

OTN provides training for all staff on how to recognize phishing and other social engineering attacks, as well as what to do if a suspicious email is received or a security incident is suspected. To date, these efforts have been fruitful in terms of identifying and responding to phishing attacks and preventing their success. As these attacks become more and more sophisticated and targeted against senior executives, OTN will continue to review, update and supplement its training materials on a regular basis.

[7] Jean Baptiste Su (2019), "Cybercriminals Favor Targeting Top Executives, Small Businesses, Money: Verizon Data Breach Report" [Online], Available: https://www.forbes.com/sites/jeanbaptiste/2019/05/11/cybercriminals-favor-targeting-top-executives-small-businesses-money-verizon-data-breach-report/#7164038f30e6 [2019, June].

11. References

Beamish, Brain (2019). “Comments of the Information and Privacy Commissioner of Ontario on Bill 74” [Online]. Available: https://www.ipc.on.ca/wp-content/uploads/2019/04/2019-03-bill-74.pdf. [2019, July].

Canadian Radio-television and Telecommunications Commission (2018). “CRTC Issues $250,000 in Penalties to Combat Malicious Online Advertising” [Online]. Available: https://www.canada.ca/en/radio-television-telecommunications/news/2018/07/crtc-issues-250000-in-penalties-to-combat-malicious-online-advertising.html. [2019, July].

Innovation, Science and Economic Development Canada (2019). “Canada’s Anti-Spam Legislation” [Online]. Available: https://www.fightspam.gc.ca/eic/site/030.nsf/eng/home. [2019, July].

Su, Jean Baptiste (2019). “Cybercriminals Favor Targeting Top Executives, Small Businesses, Money: Verizon Data Breach Report” [Online]. Available: https://www.forbes.com/sites/jeanbaptiste/2019/05/11/cybercriminals-favor-targeting-top-executives-small-businesses-money-verizon-data-breach-report/#7164038f30e6. [2019, June].

12. Appendix: PHIPA Roles for OTN by Program, Service or Pilot/Proof of Concept (POC)

OTN's roles and obligations under PHIPA may change on a transaction by transaction basis and may change or evolve based on a new program, service mandate or use case. As such, it has been OTN's practice to ensure it meets all role obligations as defined in this document for all its service offerings.

OTN Service Name	Associated PHIPA Role	Description of Roles and Responsibilities
Scheduling	Agent & eService Provider	Where OTN schedules clinical telemedicine appointments on behalf of custodians (i.e. healthcare organizations and healthcare providers) it accesses and handles PHI as an Agent. Where OTN provides the technology and IT services (e.g. scheduling tool, data centers, servers and technical support) to enable healthcare organizations and healthcare providers to schedule their own clinical telemedicine appointments, OTN acts as an eService Provider.
Videoconferencing Room-Based and Software Based	HINP & eService Provider	Where OTN provides the videoconferencing technology and IT services to enable two or more custodians to share PHI, it acts as a HINP. Where OTN provides the videoconferencing technology and IT services to enable a custodian to connect directly with a patient, OTN acts as an eService Provider. Where OTN provides iOS and Android video apps and IT services to enable two or more custodian to share PHI, it acts as a HINP. Where OTN provides a reusable Video API proof of concept as an on-going service to third-party service providers to integrate its software-based videoconferencing solution with other apps and/or solutions, it acts as an eService Provider.

OTN Service Name	Associated PHIPA Role	Description of Roles and Responsibilities
Store Forward	HINP	Where OTN provides the store forward technology and IT services to enable two or more custodians to share PHI, patient images or video files asynchronously, it acts as a HINP.
eConsult	HINP & eService Provider	Where OTN provides the technological means and IT services to enable two or more custodians to share PHI for a consultation, OTN acts as a HINP. Where OTN is providing the API libraries to integrate eConsult with provincial EMRs, OTN acts as an eService Provider.
Telehomecare	HINP, eService Provider & Agent	Where OTN provides the technology, IT services, and program training to enable patients to self-manage their chronic disease, vital signs, and/or symptoms with the coaching of their healthcare provider, OTN acts as an eService Provider. In making the Third-Party managed services available to Host Organizations, OTN is acting as an eService Provider to the Host Organizations. Where the technology is used to share PHI between HICs, and where OTN has integrated with OntarioMD's Hospital Report Manager, OTN acts as a HINP. Where OTN provides the technology and IT service (e.g. RightFax server, data centre and associated support) to enable healthcare organizations and healthcare providers to share PHI between HICs, OTN acts as a HINP. Where OTN facilitates research, evaluation and/or data analytics for this program, OTN acts as an Agent on behalf of the custodian.

Mental Health Support		
Big White Wall (BWW)	Agent & Service Provider	For the purposes of this pilot, OTN acts as a Service Provider where OTN is providing access to the BWW web application and as an Agent when facilitating research and/or data analytics.
Therapy assisted Internet Cognitive Behavioural Therapy (TA-iCBT)	Procurement Agent/Recipient	OTN acted as a procurement agent with respect to the procurement of two iCBT solutions for itself and its members. OTN acts as the sole Recipient with respect to the preparation of privacy and security assessments, audits, inspections and/or investigations.
Teleophthalmology	HINP	Where OTN provides the technology and IT services to enable HICs to share PHI for the purpose of retinal screening, assessment and the development of a treatment plan, OTN is acting as a HINP. Third-Party Managed Service: When OTN transitions this service to a third-party managed service delivery model, OTN will continue to act in its capacity as a HINP.
Secure Messaging Proof of Concept (PoC)	HINP & eService Provider	Where OTN provides secure, encrypted messaging technology and IT Services to enable two or more custodians to share PHI and coordinate or support provision of care, it acts in its capacity as a HINP. Where OTN transmits PHI to a HIC to facilitate a privacy and/or security investigation by the HIC, or to support the HIC in responding to an access request, OTN acts as an eService Provider.
Primary Care eVisits	HINP & eService Provider	Where OTN is the program sponsor and co-designer of eVisit, is responsible for the delivery model, oversight of the project and project evaluation, it acts as a HINP. For the delivery of Video conferencing (Pexip) and for Hospital Report Manager delivery of Electronic Medical Record and billing functions, OTN acts as an eService Provider.

For more information on OTNs privacy program, please visit https://otn.ca/privacy-centre/.

- Visit otn.ca to discover the full range of connected care options.
- Are you a healthcare provider? Visit OTNhub.ca to discover patient care and professional development options.
- Call us. We'd love to help you get started. 1-855-654-0888

Ontario

OTN is a not-for-profit organization
funded by the Ontario Government