PRIVACY PROGRAM

FY 2016/17 Annual Report

September 2017

Privacy as a Service

Working smart, solving problems, building trust

105 Moatfield Drive, Suite 1100 Toronto, ON M3B 0A2

PRIVACY PROGRAM
FY 2016/17 ANNUAL REPORT

TABLE OF CONTENTS

1. PURPOSE OF THE REPORT

This is OTN's third comprehensive Annual Privacy Program Report. The purpose of this report is to describe OTN's Privacy Program and highlight the privacy milestones achieved in 2016-2017. The Annual Privacy Report concludes with a summary of the key privacy initiatives for 2017-2018.

Contributions from OTN's Information Security Office, Customer Care Center, Technical Operations, Contract & Procurement Management, Adoption, Marketing/Communications and the PMO are critical to the OTN Privacy Program and are acknowledged within relevant sections of this report.

Contact

Communications regarding this document can be directed to:

Sylvie Gaskin
Director, Privacy & Risk
Ontario Telemedicine Network
t. 416-446-4110 x 5187
e. sgaskin@otn.ca

2. OTN's PRIVACY PROGRAM – WHO WE ARE

Established in 2006, OTN's award winning Privacy Program has progressed on the maturity curb from a one-person office to a virtual privacy team comprised of industry and subject matter experts that offer a suit of privacy assurance services not only to internal OTN stakeholders but also to OTN customers and partners. Our small but mighty team, strives to build strategic relationships and to create and sustain an environment that breeds continuous learning & innovation. It champions compliance driven, by design approaches and tactics that align with and support key organizational/provincial priorities.

Our philosophy at OTN is that legislation is the floor not the ceiling. That a balanced and risk based approach to privacy solves problems and removes barriers. Privacy is a Service that builds trust, breeds innovation and contributes to a positive customer/patient experience…Privacy should be the selling feature for innovative and digital health solutions.

Michelle MacMillan & Sylvie Gaskin – 'Embedding Privacy by Design into Telemedicine Inspires Trust and Adoption' – eHealth 2017 Presentation

2.1 Objectives

OTN is **committed** to **respecting personal privacy** and **safeguarding data assets** including but not limited to personal health information and personal information, that it and its third parties may handle and host on behalf of OTN customers and consumers.

"the definition of personal data in the 21st century is a 'moving target' due to the new dimensions added by advanced information communication technologies including intrusive devices, use of biometrics, social media, powerful search engines and maintenance of transnational databases" https://iapp.org/news/a/from-ancient-to-modern-the-changing-face-of-personal-data/

OTN has responded to constant changes in technology by taking strides to mature, improve, and at times re-design elements of its Privacy Program and by taking a **balanced approach** to ensuring privacy obligations and risks are met and managed on a continuous and **organizational-wide** and with a **provincial focus**.

The **changing face of the privacy landscape** and of the **healthcare ecosystem** not only requires innovative and adaptable privacy professionals that are steeped in their knowledge of global privacy laws, healthcare trends and issues, information technology, the internet of things (IoT), cloud computing, data analytics but also **new ways** of thinking and embedding privacy into everything that we do.

Our Impact – The privacy culture at OTN has been a significant contributor to OTN's brand and reputation as a world leader and trusted partner

2.2 Governance and Accountability

Given the changing face of privacy and the complex healthcare and regulatory ecosystem in which it navigates it is key for OTN's Privacy Program to have a robust foundation from which to pivot and adapt. To that end OTN's Privacy Program has an established governance structure, key objectives, services and processes.

Roles	Responsibility
Board of Directors	Holds fiduciary accountability for OTN and is responsible for the organization's compliance with the law, 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 Security.
Chief Executive Officer	Has been delegated authority to operate OTN on a day-to-day basis, implement policy, including privacy, information management policies, and risk management practices
Senior Leadership Team	Chaired by the CEO and manages the day-to-day business of OTN, approves privacy and information policies, and provides management direction on major privacy issues
VP Finance and Administration	Is the executive sponsor for the privacy program and oversees the privacy function at OTN.
Chief Operating Officer	Is the executive sponsor for the security program and oversees the security function at OTN.
Executive Lead, Technology and Deployment	Has overall responsibility for the software development, quality assurance, release management, development operations and infrastructure teams. (including Information Security Team)

Roles	Responsibility
Chief Information Security Officer	Accountable to review, audit and provide advice on our information security program against industry standards to maintain the confidentiality, integrity, and availability of all OTN information systems.
Director Development Operations and Infrastructure which includes Security Operations	Accountable for the Information Security Program at OTN and for the security of OTN information systems.
Director Privacy and Risk	Oversees and leads all aspects of OTN's privacy program and provides privacy, risk, policy and compliance leadership to a variety of stakeholders both internal and external to OTN.
Security Officer/Analyst/Engineer	Are responsible for managing the security of OTN information systems, reviewing audit logs, and for conducting Threat and Risk Assessments
Privacy Specialists – Privacy & Risk Officer	Are responsible for providing privacy assurance services to OTN projects, conducting privacy impact analysis, investigating privacy incidents, and other related responsibilities.
Privacy & Security Lateral Team	Is chaired by the VP of 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 Program and to direct the requirement for broader organizational consultation when needed.

2.3 Privacy Assurance Services

OTN Privacy Operational Plan

On an annual basis the privacy team identifies key operational objectives. The privacy operational plan is aligned to key strategic organizational and provincial priorities and informs individual team plans.

OTN Privacy Policies and Procedures

OTN has established a comprehensive suite of privacy policies to guide its privacy culture and program. A number of new policies have also been identified for creation & inclusion in OTN's Privacy Policy Framework. The framework triggers review dates to keep policies up-to-date and current.

Monitoring and Compliance

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

1) Incident reporting and investigation tools
2) Risk identification and mitigation strategies via Privacy Impact Assessents (PIAs), Threat and Risk Assessments (TRAs) and Privacy and Security Architectures (PSAs)
3) Privacy scorecard & product specific privacy scorecards
4) Privacy Risk register
5) Compliance & monitoring policy and reporting tool
6) Mandatory staff orientation and training
7) Policy/guideline review process
8) Inquiry tracking & trending

Privacy Incident Management

OTN has implemented a Privacy Breach policy and procedure which outlines the following situations that trigger a privacy investigation & escalation process:

- There has been an unauthorized disclosure of PHI; PI or confidential information or
- There is a suspected unauthorized disclosure of PHI; PI or confidential information or
- A person unauthorized to do so, has accessed PHI, PI or confidential information either accidentally or intentionally; or

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

Responsibility for investigating and documenting the findings of any situation described above is triaged by the Director of Privacy and Risk to a member of the privacy team as appropriate.

There is a detailed escalation and notification process based on incident severity.

Because OTN is a Health Information Network Provider (HINP) and not a Health Information Custodian (HIC), OTN does not directly notify patients of privacy breaches involving patients.. Information is passed on to the HIC or HICs with affected patients, who will then notify patients in accordance with their own incident management procedures and requirements.

Where appropriate, opportunities for improvement are identified and recommended to applicable stakeholders.

Privacy Training – Awareness for OTN Employees

OTN has implemented comprehensive privacy training opportunities for its employees. The privacy training offerings, educate OTN employees, contractors, and third parties on privacy and information security principles, policies, procedures, and guidelines. OTN delivers the training and awareness in the following four ways:

1. All OTN employees participate in privacy training using OTN's Privacy learning on-line module. The privacy module consists of numerous privacy lessons (covering privacy, PHIPA, roles/responsibilities, handling of confidential information, and detecting breaches) and a quiz. Privacy training is mandatory and is to be completed by all staff within 4 weeks of their start date.
2. All employees are introduced to their privacy obligations during OTN's new employee orientation.
3. Customer Care Centre staff complete privacy training within 2 weeks of their start date and must also complete additional enhanced privacy training which is also to be completed within 2 weeks of their start date. This includes learning the policies and procedures directly relevant to them.
4. From time to time, OTN executes poster campaigns and privacy awareness and education campaigns. These campaigns include Blogs and/or articles in the "OTN Update" newsletter.

Privacy Awareness for OTN Customers and Members

OTN's Privacy Team works collaboratively with OTN's Training Team & other service areas to ensure that they are actively responding to the learning needs of customers . Offering both new and existing customers training sessions through various modalities, the OTN Privacy Team assists customers achieve consistent, effective, and quality privacy learning.

Training for customers **is a critical success factor** for ensuring the privacy of PHI in a complex and dynamic virtual healthcare environment.

To that end, the privacy team is in the process of refreshing and updating all of its privacy awareness/training artifacts and building member facing and consumer facing awareness modules.

Privacy Scorecard – Metrics & Reporting

OTN has a number of metrics (i.e. # of incidents investigated, training completed, # of closed risks) it documents by way of a privacy scorecard; tracked and trended over time. The scorecard in its entirety is reported to OTN's Privacy and Security Lateral Team (PSLT) with some key indicators reported corporately to the Senior Leadership Team as well as at the Board level.

PIAs & Risk Register

A Privacy Impact Assessment (PIA) is a risk management tool that allows OTN in its role as a Health Information Network Provider under the *'Personal Health Information Protection Act, 2004'* to assess a technology, program or information system's privacy risks and its compliance with provincial and federal legislative requirements and standards.

Where required, a PIA also details mitigating strategies by way of recommendations and an action plan. **A critical element of the PIA process is the implementation of the recommendations detailed in the assessment**.

PIA summaries are **shared** with OTN members/users and **published** on OTNhub.ca.

A PIA has the benefit of generating and communicating with confidence that privacy requirements have, or are being met and what risks have or are in the process of being mitigated. A PIA is meant to be used and expanded over the cycle of the initiative's development and implementation. PIA's are refreshed over time to continuously identify and address risks that have the potential to impact the confidentiality, integrity and accessibility of personal health information held/handled by OTN and/or its partners. OTN has adopted a risk tolerance level of low, meaning that low and very low risks will not be

immediately actioned, but will be monitored to ensure that they stay within tolerable levels. All high and medium risks are actioned and mitigated to an acceptable level.

The privacy program has also established a privacy risk register to document, track and monitor risks & recommendations identified via PIAs. Those risks are reported to the PSLT as part of the privacy scorecard metrics.

Consultation Services

The privacy program responds to internal and external inquiries on a variety of privacy topics and issues related to privacy in a digital care environment. The privacy program also provides a number of privacy assurance services to OTN's project management office (PMO), other OTN business functions and programs as well as external stakeholders as required.

2.4 Policy Office

Although not a traditional role for the Privacy Team, given its expertise with privacy policy management it provides oversight, support and tracking for all of OTN's 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, regulatory and governance requirements, to protect OTN and its stakeholders, and to guide change where necessary. Of the **152 policy documents** currently in place **75%** (114) are current and up-to-date. A plan is in place to continue updating policy documents that have reached their review period.

Types of Policy Document	Total # of Documents	Documents Archived in 2017	Under Review by Portfolio as of Sept 2017	New documents Under Development
Policy	52	0	7	1
Policy & Procedure	56	2	14	1
Guidelines	20	3	13	1
Standard	1	0	1	
Resource (e.g. forms)	22	0	7	2
Total	152	5	37	5

3. OPERATING PLAN

OTN's Privacy Program is an award winning and internationally recognized program. As such and in order to continue building 'trust', remove barriers and find solutions, OTN's Privacy Program needs to stay current, drive innovation and raise the bar of privacy excellence, even if ever so slightly.

Highlighted below are strategies and initiatives the Privacy Program is currently leading and executing to plan to ensure that OTN is not lagging from a privacy foundational and maturity perspective. The planning, engagement and implementing phases for some of these initiatives began in 2016 but were completed or near completion in FY 2016-2017.

3.1 OPERATING PLAN 2016-2017 – A YEAR IN REVIEW

Objective	Activity
Touch Point with Information and Privacy Commissioner of Ontario (IPC)	Face to face meeting between OTN's privacy program team & the IPC Ontario to review privacy program and OTN's evolving role
CASL Compliance Phase 2	Transition OTN to express consent model to transmit CEMs to customers • CRM • Marketo • Sign-up form (solo-org) • CASL policy legal review – in progress
Privacy Policy Framework	Role Based Access Policy • Mapping of all employee access roles for all OTN applications • Remedy new hire form for People Leaders
Privacy Learning Program Facelift	Based on lessons learned content created for the following: • PMO privacy awareness module • Member facing privacy awareness module • Consumer facing privacy awareness module – underway • Presentations delivered to 7 Telemedicine Coordinator Forums

4. PRIVACY ASSURANCE AND RISK MANAGEMENT

Privacy assurance & risk management is one of the key services provided by the privacy team to ensure OTN programs, services and projects comply with applicable legislation and standards and meet customer and patient expectations.

You can't manage or improve what you don't know. You can't fix what you don't acknowledge.

The Privacy team is involved with OTN's Gating Process and Project Management Lifecycle Methodology to pre-emptively identify/mitigate any risks and ensure that privacy considerations and safeguards are embedded into each step of the project's design and delivery.

This approach **drives innovation**, **reduces costs** and **prevents last minute re-work and project delays**. Furthermore, it **shapes trust and confidence** that OTN services and programs will **not only improve access to care** but also afford customers and patients a **privacy positive experience**.

The privacy team provides the following services to support privacy assurance and risk management:

- Privacy consultation
- Privacy Threshold Assessments
- Privacy Impact Assessments (PIAs) & mitigating plans
- Privacy and Security Architecture design documents
- Statement of Risks documents
- Subject-matter expertise (SME) contribution to architecture, solution design/interface, change management and business requirements documents
- SME contribution to RFI, RFP and SOW documents and processes
- Language for and review of agreements & MOUs
- SME contribution to privacy communication & training materials
- Development of and updates to privacy, security and other relevant policies and procedures

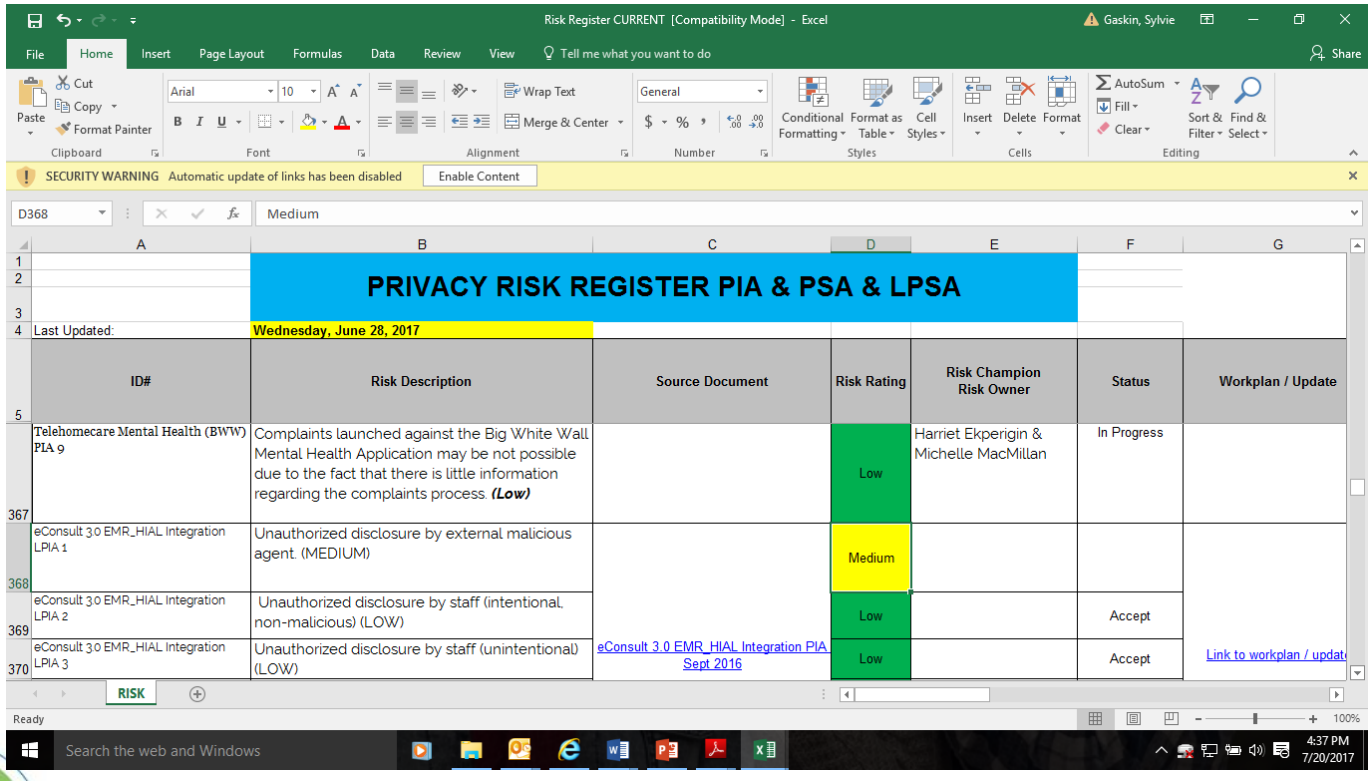
- Consultation with IPC, legal counsel & other external partners as required

Initiatives led or supported by Privacy & Risk Team 2016-2017

Privacy Assurance Service	Project		Total
Privacy Impact Assessments (PIA)s led by external consultants with oversight from OTN's privacy specialists	• Federation • Teleophthalmology • Video API • BWW		4
Internal Privacy Review or Statement of Risk conducted by OTN privacy specialist	• Store Forward Medweb IOS App • eConsult Managed Service • OTNInvite Clinical Multipoint • TSM 6.7 Join a Call		4
Other Privacy Assurance Services delivered to the following initiatives and projects	Data Governance Framework Customer Registration Intake Pathway Practical Apps Secure Messaging Android 1.2 Customer Registration Contracts Webcast Center THC New Pt. Group CKD Federation Teleophthalmology OTNInvite Clinical Multipoint PMMS 2016 OTNhub redesign Customer Registration Order Processing	Directory Directory 3.2 eConsult Phase 1 eConsult Phase 2 New CRM requirements Solution Formulary OTN.ca redesign Sign-Up Form Phase 1 Sign-Up Form Phase 2 CKD THC New Pt. Group Diabetes THC New Pt. Group Mental Health Sf Medweb IOS App Video API TSM 6.7 Join a Call OTNhub 1.6	30

5. PRIVACY IMPACT ASSESSMENT – FINDINGS

OTN's Privacy Impact Assessment (PIA) policy and general practice is to **mitigate** all **medium** and **high risk findings** associated with its projects, services and programs, prior to the launch of a new project or initiative or prior to a new release or upgrade. In FY 2016-2017, 11 high risks and 10 medium risks were closed. There are currently 6 high risks (see appendix below) and 35 medium outstanding risks being monitored and tracked by the privacy team, that though important and still needing to be addressed, are risks OTN management accepted as they are being managed and/or monitored by interim measures. As noted earlier, summary findings of OTN PIAs are shared with customers and published on OTNhub.ca.



6. PRIVACY INVESTIGATIONS AND BREACHES

A key component of and requirement for OTN's privacy assurance & risk management services is the identification, reporting, management and resolution of reported privacy incidents and breaches. Privacy incidents and breaches in a telemedicine/digital care environment occur when there is unauthorized access, collection, use, retention, disclosure or disposal of patient information either by OTN or its members. Incident reporting is an agreed upon role and responsibility between OTN and its members/users.

As you can see in the table below, in 2016-2017 the Privacy & Risk team saw **a slight increase** in the total number of **reported privacy incidents** from 87 the previous year to 89 this past fiscal. The number of incidents identified as **breaches also increased slightly**, from 25 in 2015/2016 to 28 in 2016/2017. If we examine the trends in the table below we can attribute some of the increase with OTN efforts to augment the number of sites/users that can self-schedule videoconferencing events and with the launch of one of its Telehomecare pilots.

With **new mandatory breach reporting requirements coming into effect in October 2017** for members/users the Privacy Team continues to **drive privacy best practices** and **improvement opportunities** through awareness, training, privacy by design opportunities and product releases.

Privacy Investigations	2012-2013	2013-2014	2014-2015	2015-2016	2016-2017
Total # of Incidents Investigated	101	81	92	87	89
Total # of breaches	50	64	40	25	28
OTN Action	33	32	19	12	13
Member Action	12	30	19	12	13
OTN and Member Action	5	2	2	1	2
Breaches High Severity	0	0	0	0	0
Breaches Medium Severity	4	0	1	0	1
Breaches Low Severity	46	64	39	25	27

Following a privacy investigation, the privacy team works with its members/users and internal product/service subject matter experts to recommend and **drive privacy best practices** and **improvement opportunities** to **prevent future breaches**.

Privacy breaches by product/service

There are over 600,000 + telemedicine events and/or services held/delivered using OTN videoconferencing solutions. Videoconferencing and scheduling related human errors remain the main source of privacy breaches reported.

Breaches by Product/Service	2012-2013	2013-2014	2014-2015	2015-2016	2016-2017
Room-based videoconferencing	41	52	25	16	8
OTNhub	n/a	n/a	n/a	n/a	2
eConsult/SF	8	5	3	2	2
Personal Videoconferencing	0	3	4	1	2
TSM/Ncompass	0	0	3	4	10
Telehomecare	0	0	0	0	2
Teleophthalmology	0	1	2	0	0
Webcasting	1	3	3	2	1
Emergency Services	0	0	0	0	0
Learning Center	0	0	0	0	0

Breaches by Product/Service	2012-2013	2013-2014	2014-2015	2015-2016	2016-2017
Other	n/a	n/a	n/a	n/a	1
Total	50	64	40	25	28

7. CANADIAN ANTI-SPAM LEGISLATION (CASL)

The 'Canadian Anti-Spam Legislation' (CASL) creates an "opt-in" regime for commercial electronic marketing, and amends four federal statutes: the Canadian Radio-television and Telecommunications Commission Act (CRTC); Competition Act; Personal Information Protection and Electronic Documents Act (PIPEDA); and Telecommunications Act.

In general, CASL requires express or implied consent for the sending of "commercial electronic messages" and installation of a computer program in the course of commercial activity.

The first of three phases (i.e. sending of commercial electronic messages) of CASL came into effect on July 1st 2014. At that time and as permitted by CASL, OTN relied on an implied consent model leveraging existing business relationships with customers/members and proper unsubscribe functionality to manage commercial electronic messages (CEMs) i.e. marketing/promotional communication.

On July 1, 2017, CASL's express consent requirements came into effect. The private right of action was however suspended.

OTN has put in place the following measures to comply with those new express consent CASL requirements:

- **Express consent campaign** (during June) to **existing** OTN members/customers seeking/documenting their express consent to continue receiving OTN email marketing/promotional communication
- Starting in July, **new organizations and individuals** were prompted for their express consent during OTN's sign-up form registration and first login processes via the OTNhub
- All consents & unsubscribe requests will continue to **be tracked and managed centrally in Marketo** by the **Marketing/Communication team**
- OTN's CASL **policy is being reviewed/updated** by OTN's legal counsel (BLG)

CASL Fines and litigation – For reference and as a reminder only

Contravention of CASL's CEM rules can result in**:**

(1) potentially severe administrative monetary penalties (up to $10 million per violation for an organization and $1 million per violation for an individual) in regulatory proceedings; and

(2) As of July 1, 2017, CASL contraventions are **subject to enforcement through private litigation**, including class proceedings, by individuals and organizations seeking compensatory damages.

CRTC

The Canadian Radio-television and Telecommunications Commission ("CRTC") has regulatory and enforcement authority for CASL, and continues to investigate a significant number of reported violations; 950,000+ and the number is expected to continue to increase. Many of the submissions are as a result of:

- Consent violations
- Ineffective and non-functional unsubscribe mechanism
- Prescribed formalities and sender Contact Information

CASL compliance although detailed and complex is another opportunity for OTN to connect with and build a trusted, knowledgeable and respectful relationship with its members/users

8. OPERATING PLAN 2017-2018

A LOOK FORWARD – STAYING ONE STEP AHEAD

Highlighted below are strategies and initiatives the Privacy Program will be leading in 2017-2018 and executing to plan. As noted earlier building trust, breeding innovation and positioning **Privacy as a Service** to OTN and the Healthcare Community requires a strong foundation, continuous outreach, learning, change management and the occasional pivot.

Objective	Activity
CASL Compliance Phase 2	Transition OTN to express consent model to transmit CEMs to customers • Sign-up and consent org model • CASL Policy
Privacy Learning Program Facelift	• PMO privacy awareness module • Member/user facing module with tips and recommendations based on lessons learned • Consumer/patient facing module with tips and recommendations based on lessons learned and IPC of Canada resources • Presentations delivered to multiple Telemedicine Coordinator Forums
Privacy re-design for Marketplace	• Re-design of privacy touchpoints for innovative procurement • Dynamic assessment privacy/security questionnaire for vendor community • Library of controls/requirements • Privacy & Security for Marketplace Final Report • Marketplace Privacy & Security Guide for Innovative Procurement
Legal Authority and Framework Review – Data Assets	Engagement with Deloitte to conduct • conceptual privacy impact assessment • environmental scan • current state review of data assets/legal authority and framework • future state regulatory analysis • recommendations/road map & implementation plan to address OTN's evolving role

9. TRENDS SHAPING OTN

The Privacy team strives to create and sustain an environment that breeds continuous learning & innovation and champions strategies and tactics that align with and support key organizational and provincial transformational initiatives.

In addition to internal and provincial alignment, OTN's Privacy Program must also be forward looking and aware of local/global trends for which OTN needs to consider, adapt for and integrate into its business plans and practices.

The following are key **trends shaping OTN and for the Privacy Team** to consider and /or plan for in order to support OTN to successfully achieve its 2017-2018 key objectives:

- Marketplace
- Cloud Migration
- Member Customer Self-Management
- Integration with & Leading Provincial Assets
- OTN data assets – current and new role
- Information Security

Marketplace

OTN is **transitioning** to a multiple vendor/marketplace environment and in some cases to a third party managed services model. The digital health marketplace and other OTN teams are exploring data warehousing opportunities. The Privacy Team in collaboration with the Marketplace team engaged Deloitte to redesign privacy touchpoints that align with innovative procurement and the digital health marketplace approach and processes.

Privacy has shifted from being application centric to platform/cloud/interface centric. Privacy requirements, controls, risk assessments, templates, processes, procurement, legal frameworks and reporting also need to accommodate this shift.

More and more the Privacy Team is providing Privacy as a Service to the vendor community where privacy programs may not be as mature as required **to empower** healthcare organizations, partners and providers to deliver **privacy mature/compliant and secure** virtual healthcare to their patients.

Cloud Migration

In anticipation of everything 'Cloud' a few years ago, the Privacy Team in collaboration with the Information Security Team **proactively** engaged a third party to assist in developing a **Cloud Computing Framework and Cloud Policy for OTN**. As OTN transitions some of its operations to a cloud environment and to third party vendor cloud hosted applications it is considering/assessing its broad organizational readiness to support this migration. From a privacy lens the following are key considerations:

- Agreements and privacy controls need to reflect SaaS, PaaS
- Risk assessments must move to cloud focused PIAs/TRAs
- Oversight/governance must be in place for cloud hosted OTN and Third Party Managed Services including data assets
- Audits must be in place to harmonize agreements and vendor compliance
- Operations must transition to a cloud environment

Member & Consumer Self-Management

As OTN **shifts** to a more **member self-management** and **direct to consumer self-registration model and approach** it is key that both have a positive and seamless privacy experience while using digital health solutions. As such OTN's Privacy Team is developing privacy learning artefacts (short tips and best practices) geared to help healthcare professionals and individuals deliver and/or receive healthcare in a digital environment. **Privacy** must be **a Service** to both the **healthcare community and to patients/consumers.**

Integration with & Leading Provincial Assets

As OTN continues to impact the delivery and access to care by working with provincial partners and enabling the spread and scale of provincial programs and digital care solutions, the Privacy Team is **taking a lead role** in ensuring privacy requirements, standards, controls and processes have a provincial focus, consulting with the IPC and legal counsel and ensuring that agreements clearly detail the privacy/security roles, responsibilities and expectations of all parties. The Privacy Team is currently **leading** a third-party engagement/**review of OTN's legal authority and framework** related to the **management of data assets as its provincial mandate evolves.**

OTN data assets – existing and new role

As noted above, OTN wants to ensure the **legal authority and framework it requires** to manage its data assets **align with and supports its current and evolving role**. To that end, a conceptual privacy impact assessment and privacy authority analysis is being conducted by a third-party vendor. The privacy legal **gap assessment** will include **current PHIPA authorities** and OTN's expanding mandate, evaluating privacy legal options and privacy/governance **impacts of OTN's future state.**

Information Security

As data protection legislation and penalties get tougher in both Canada and the EU; as the volume of connected devices (50 billion connected devices and 25 million apps by 2020) and the volume of data (big data) accessible through the IoT and from other sources explodes and as cyber-attacks get smarter and continue to target healthcare organizations **it is key** that OTN **continues to mature and invest in its privacy/security culture** and that the Privacy Team work in lock step with the Information Security Team.

APPENDIX

Note that although our normal practice is to mitigate all high risks prior to project launch, these high risks, though important and still needing to be addressed, were risks OTN management accepted in the interim as not significant enough to stop a go-live on the respective projects.

Summaries of risk findings are published and shared with OTN members/users.

Privacy Impact Assessments					
6 High Risks Outstanding					
Source	**Risk**	**Recommendation**	**Action**	**Status**	**Estimated Closed Date**
Telehomecare (THC) expansion PIA Critical Dependencies	There is a risk of errors with the authentication/ credentialing practices which could result in unauthorized access to PHI.	OTN should transition THC manual authentication/ credentialing practices to OTN's automated IAM practices.	IAM automated processes and systems have been implemented for PCVC. THC continues to leverage its own user registration/onboarding processes January 2014	User credentials are created in the solution directly.	Implement the OTN Identity and Access Management System prior to full production rollout. This risk will be addressed/closed shortly with the transition to the new PMMS solution
IAM as a service PIA 2	The use of multiple sources of identity, i.e. Novel and AD,	Adhere to ISO standards on Identity Management regarding the governance,	Architecture team will work towards an integrated data model. Product team will try and	Enterprise identity model is in the works. Provincial integration	TBD not known at this time

	in addition to CRM.	policies, processes, data, and technology.	align strategy with provincial identity management solution.	strategy is still in very early discussion stages with eHealth Ontario. No Timing from business.	

Source	Risk	Recommendation	Action	Status	Estimated Closed Date
PCVC Send Invite 1.3 (formerly Guest Link) PIA 2	Lack of documentation to support compliance with ONTARIO REGULATION 329/04 of Personal Health Information Protection Act, 2004 (PHIPA	Prepare and make available: 1. Plain language description of services and safeguards 2. Plain language description of the services that the provider provides to the custodians & appropriate for sharing with patients	Working on draft Services & Safeguard documents. Meeting with Communications Team scheduled for April '16 to review and identify requirements so they can be put into a Workplan and assign timelines based on priorities.	In Progress Awaiting the Communications Team to send us the template for the Services @ Safeguard document. Due to changes in the Communication Team the deliverable will be delayed.	September 30, 2016 – A complete refresh of the PIA/TRA for PCVC is underway. A Service and Safeguards document will be designed/completed and published by Q3 2017/2018
THC PMMS to HRM Integration Solution PIA 7	No formal process in place to perform ongoing monitoring and review of audit logs, nor is any proactive monitoring of logs currently performed	Develop an inventory of systems /applications that are integrated with the SIEM and identify any gaps as it relates to OTN's critical systems. Finally, identify which systems and applications are currently encrypted, and flag those where encryption is required.	OTN has implemented the audit monitoring solution, An action plan is in place and we have use cases to detect anomalies	In Progress	Next Fiscal; 2017/2018.

Source	Risk	Recommendation	Action	Status	Estimated Closed Date
OTN Federation PIA 8	Without privacy audit procedures that clearly define the requirement of both OTN and its member organizations to conduct active reviews of OTN privacy audit logs, there is a risk that instances or patterns of unauthorized activity will not be detected by OTN or its member organizations.	The HINP should be able to log and audit all access to PHI in the system including: * who accessed the information; * the date and time of access; * what PHI was viewed; and * whether PHI was altered, deleted or transferred. References: * O. Reg. 329/04, s. 6.(3)4.	Security is working on a Desired State, this has a dependency on OneID, which currently doesn't have a definitive answer: With the help of Titan Plus Software and the MSSP, appropriate log levels will be configured on the NetIQ infrastructure to log events of interest and having them shipped to a central location (MSSP) for correlation, monitoring, alerting and retention.	In Progress	Next Fiscal 2017-2018
SF Medweb iOS APP Risk 7	Roles and responsibilities including liability and/or privacy and security language with respect to the Medweb App are not defined and may expose OTN and App users to undue risks	Augment OTN consolidated agreements with language associated with OTN built/branded Apps. Include Privacy Notice similar to that for the iOS Vidyo App.		In Progress	Q1 2017-2018