Privacy Program

FY 2017/18 Annual Report

November 2018

Privacy is the New Currency

Care. Connected.

Table of Contents

1. PURPOSE OF THE REPORT

This is OTN's fourth comprehensive Annual Privacy Program Report. The purpose of this report is to describe OTN's Privacy Program and highlight the privacy milestones achieved in 2017-2018. The Annual Privacy Report also includes a summary of the key privacy initiatives for 2018-2019 and trends that we are either involved in or monitoring.

Collaboration with OTN's Senior Leadership Team, Information Security Office, Member Services Team, Technical Operations, Contract & Procurement Management, Adoption, Marketing/Communications, the Project Management Office and many others, are critical to the success of OTN's 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 – OBSERVATIONS & WHO WE NEED TO BE

Whether you personally believe privacy is important or not, one cannot watch the news, read blogs or surf the internet without seeing one of the following headlines weekly if not daily: 'Privacy is the new green and trust is the new currency', 'Privacy is the new money', 'Digital trust of health information is a privacy currency', 'Privacy is not a currency', 'Facebook lost approximately $150 billion U.S. in two hours' over its privacy and security practices'.

The pervasive impact of privacy gone wrong and the various views on the same general theme are striking. As individual members of society and recipients of healthcare in some capacity, these themes and issues resonate. More than ever, our identity, health & personal information has become the new currency, as we routinely hand over that information in exchange for convenience, social media and on-line services. More than ever we should consider what and how much information we are willing to give up.

"Now consumers are starting to shift back in the other direction, holding their privacy closer to the vest. Many are realizing that their privacy is a high-value currency, critically assessing how, when and where they're willing to spend that currency".

Data is Currency, Don't Abuse It

In an organization committed to be a strategic and trusted partner, delivering and guiding pan-provincial digital health services, we more than ever need to be aware that there is a growing shift in the privacy paradigm. Privacy is the new currency - no matter what side of that coin you might be - which inherently will mean different things to Ontarians, funders, healthcare providers, healthcare organizations and vendors.

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. This is comprised of industry and subject matter experts that offer a suite of privacy consultative and assurance services, not only to internal OTN stakeholders, but also to consumers, customers, their patients/clients and our partners. Our 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 and provincial priorities, regulatory changes, national and international trends in data privacy and cyber security.

Our privacy program's philosophy is that legislation is the floor not the ceiling. That a balanced and risk-based approach to privacy protect individuals, solves problems and removes barriers. Privacy is a Service that builds trust, breeds innovation and contributes to positive digital health experiences and outcomes. Privacy should be the selling feature i.e. the new currency for innovative and digital health solutions.

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, its third parties and partners may handle and host on behalf of OTN customers and consumers.

OTN responds to the fast past and constant changes in technology by taking strides to continuously 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 ongoing changing face of the privacy landscape and of the healthcare ecosystem not only requires innovative and adaptable privacy pros (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.

The privacy culture at OTN remains a significant contributor to its brand and reputation. As we support and enable existing and new business models, we are committed to doing so without compromising individual privacy.

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 and accountability 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 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	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	Led by the CEO, manages the day-to-day business of OTN, approves privacy and information security policies, and provides senior management direction on major privacy and information security 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 senior executive accountable for overseeing the Information Security Function at OTN.
Executive Lead Platform Redesign	Executive Lead at OTN responsible for DevOps and Infrastructure which includes the Information Security Function

Roles	Responsibility
Director Dev Ops and Infrastructure which includes & Information Security Operations	Accountable for the Information Security Function at OTN and for the security of OTN information systems.
Manager Information Security	Responsible for Managing the Information Security activities at OTN
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. Accountable to review, audit and provide advice on information security program against industry standards to maintain the confidentiality, integrity, and availability of all OTN information systems. Most Responsible Person for Business Continuity Processes
Manager Privacy	Responsible for Managing privacy program activities at OTN
Security Officer/Analyst/Engineer	Are responsible for managing the security of OTN information systems, investigation security incidents, reviewing audit logs, and for conducting Threat and Risk Assessments
Privacy Specialists	Are responsible for providing privacy assurance services to OTN functional areas and projects, conducting privacy impact assessments, 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.

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.

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 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.and are required to complete an annual refresher.
3. Member services and PMO 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 continuously refreshes and updates all of its privacy awareness/training artifacts and builds member facing and consumer facing awareness artefacts. Recently an awareness module was created to support OTN's direct to consumer services available at myvirtualhealth.ca.

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.

Privacy scorecards by product line have been developed to inform product and project managers on key privacy metrics and improvement opportunities for their product road map..

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.

2.4 Policy Office

Although not a traditional role for the Privacy Team, given its expertise with privacy policy management, it does provide 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. Last year, OTN had 152 policy documents in place with 72% (110) current and up-to-date; 3 were archived and 3 new policy documents were published. There are now 154 policy documents in place with 61% (93) being current and up-to-date.. Policy owners are prompted through automated notifications 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.

Retention and destruction schedule for sensitive and other key OTN records is also maintained by the Privacy & Risk Program to ensure retention, archiving and destruction practices are consistent and aligned with industry standards.

3. OPERATING PLAN

Highlighted below are key strategies and initiatives the Privacy Program led and executing to plan to ensure that OTN is not lagging from a regulatory or privacy foundational and maturity perspective. The planning, engagement and implementation phases for some of these initiatives began in 2017 but were completed or were near completion in FY 2017-2018.

3.1 Operating Plan 2017-2018 – A year in Review

Marketplace/Venture Development

After more than a decade of innovation, OTN is a global leader in telemedicine. OTN's programs and services were developed with providers and partners in every part of Ontario's healthcare system. The result has been improved access to care, more efficient delivery of care, and more effective collaboration between providers. The culture of Privacy & Security at OTN has been a key contributor to OTN's brand and reputation as a trusted partner and world leader in telemedicine and trusted partner.

OTN as a Marketplace for innovative virtual healthcare solutions is a new business approach/model for OTN which, to succeed, must harness and respect that world class brand and reputation. A framework and dynamic evaluation process and tools were needed to ensure OTN maintains that world class brand and reputation and to ensure healthcare organizations and providers are able to confidently, seamlessly and effortlessly embed innovative solutions into their work flows and business processes. Likewise, consumer focused solutions must empower patients to intuitively self-manage and direct their care in a manner that respects their privacy rights and safeguards their information.

In response, the Privacy and Security teams led engagement with external consultants to design and construct of a framework, tools and processes that would enable and level set innovative digital health solutions in terms of privacy, security, and interoperability readiness in order to be accepted to the OTN Marketplace.
Part of the engagement was to create a requirements library that the privacy and security teams could leverage to inform requirements for innovative procurement and/or projects.

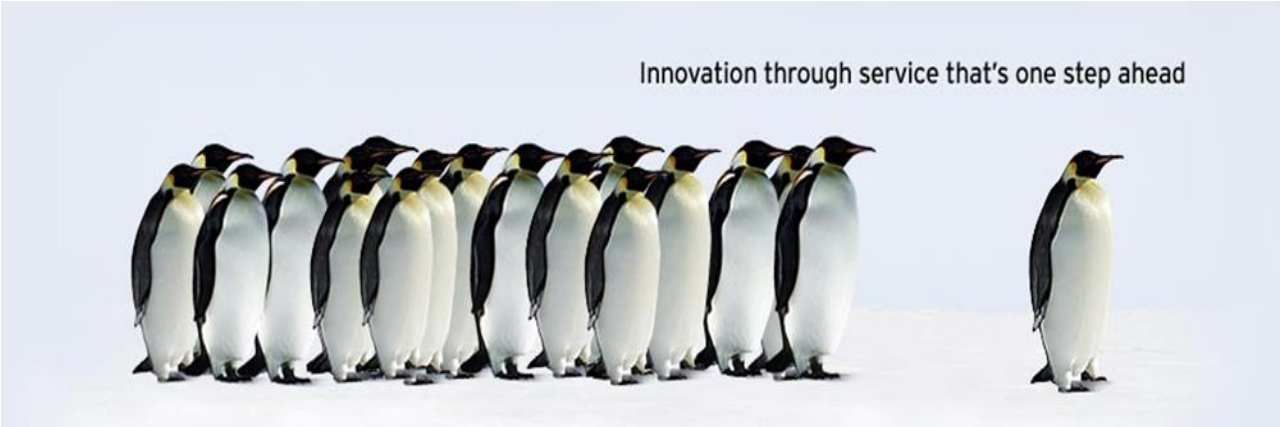
Furthermore, a privacy and security framework, tools and processes were designed and built to support OTN's marketplace/venture development opportunities and to ensure our practices remain open, transparent and robust yet agile, simple and manageable for all parties. The Privacy team continues to work closely with the venture development team as that business model and services evolve.

Authority and Legal Framework Conceptual PIA for use of OTN data

As OTN's role and mandate evolves it must ensure that it continues to have a clear legal authority, mandate, roles and responsibilities and agreement framework to optimize and manage its data assets and meet its reporting and evaluation obligations to the Government of Ontario.

As such OTN and its Privacy and Risk team led an engagement with external consultants to conduct a conceptual privacy impact assessment ("CPIA") review and analysis of the current, evolving and future state of its enterprise and privacy data management practices including those required for its Marketplace/Venture Development, Analytics, and the Marketing/Communication teams. Recommendations from this engagement will help OTN determine if it has the requisite authority, privacy governance, policies and controls, legal framework, and data governance and management practices to ensure regulatory compliance and to meet its evolving mandate.

3.2 Operating Plan 2018-2019 – A Look Forward – Innovation Through Service That's One Step Ahead



Highlighted below are strategies and initiatives the Privacy Program will be leading in 2018-2019 and executing to plan. to ensure OTN stays one step ahead and current as its role, mandate and services evolve. As noted earlier building trust, breeding innovation and positioning ***Privacy as a Service*** to OTN and to the Healthcare Community requires a strong foundation, continuous outreach, learning, change management and the occasional pivot.

Direct-to-Consumer Services – Privacy Policy Framework

Today when OTN builds and/or procures applications and/or delivers programs and services it does so predominantly in one of two roles established under the regulations made under PHIPA (Regulation). OTN is either a person providing the electronic means to each Health Information Custodian (HICs) as a Service Provider, where Custodians use the application to collect, use of disclose personal health information (PHI) for example from/to a patient or is a health information network provider (HINP) where the application is used by two or more Custodians to disclose PHI to one another.

In both roles, the PHI and other information that OTN has access to or collects (for the registration of members and their authorized users) belongs to the Custodians. The PHI to which OTN has access for the purpose of providing its services to Custodians remains in the custody and under the control of the Custodians.

OTN's practices, documentation, legal and policy frameworks is accordingly directed to Custodians and reflects the limitations and obligations imposed on Service Providers/HINPs under the Regulation.

Where OTN delivers services ***directly to Consumers***, such as Big White Wall and myvirtualhealth.ca, most of the Services will not be subject to PHIPA or given OTN is a not-for-profit organization, any other privacy law applicable law in Ontario. In the ***direct to consumer model***, OTN ***is the data steward*** of personal information rather than a service provider to Custodians. For clarity providing these service does not make OTN a health information custodian but the personal information it will collect, use and disclose in the course of providing direct to Consumer services ***will now be for OTN purposes and to connect consumers to OTN services and to external services.*** As such OTN must tailor its privacy program to include the management of consumer personal information, new or revised policies, practices and open/transparent notices. The privacy program is leading an engagement with external consultants to review its current privacy policy framework and artefacts and recommend new or updated policies, notices or practices.

Data Governance and Regulatory Framework

OTN has previously invested in two consulting engagements related to the management of its data assets:

1) Deloitte 's review and Conceptual Privacy Impact Assessment of OTN's 'Legal Authority' to use current member, patient, consumer data and environmental scan and jurisdictional review of potential strategies for future uses of those data assets (2017) and
2) KaraOne's review of OTN's data governance maturity and effective management of its data assets and corresponding activities (2016)

These key activities combined have yielded a number of recommendations which OTN has deemed to be a priority. The Privacy & Risk and Data Governance teams have partnered to put forward to OTN's Enterprise Business Office Steering Committee a business case to support a priority project that will focus on designing a data governance framework and regulatory framework tailored for OTN.

This project will ensure that OTN has the policies, processes and tools in place to optimize the value of the rich data sources OTN either currently hosts or has potential to access or create through its evolving business models, while also ensuring that the enhanced risk associated with these new models is mitigated and navigated. OTN's ability to unleash the power of data and to impact the rate at which digital health expands in Ontario will be directly proportional to OTN's ability to create/apply business intelligence from data to change the way OTN and the healthcare system delivers smart healthcare.

This project is primarily a value proposition for OTN as it will increase its ability to define telemedicine data standards, leverage data (member, consumer, vendor, partner and patient data) to make informed decisions, evaluate and improve product and services offerings, meet its TPA reporting and evaluation obligations to the MoHLTC, other funders and partners while clearly and easily understanding and meeting its regulatory and legal obligations.

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, patient and partner expectations.

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 instills trust and confidence that OTN services and programs will not only improve access to care but also afford customers, patients and other key stakeholders a privacy positive experience.

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

- Privacy consultation with the SLT, project teams, vendors and partners
- 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 and other legal artefacts such MSAs, Terms of Service, Data Sharing Agreements, Notices, Privacy Statements etc.
- SME contribution to privacy communication & training materials
- Development of and updates to privacy, security and other relevant policies and procedures
- Consultation with Information Privacy Commissioner (IPC), legal counsel & other external partners as required

Initiatives led or supported by Privacy & Risk Team 2017-2018

Privacy Assurance Service	Project		Total 2017/2018	Total 2016/2017
Privacy Impact Assessments (PIA)s led by external consultants with oversight from OTN's privacy specialists	• EAPC Novari phase 1` • EAPC Novari phase 2 • EAPC TRC Reach phase 1 • EAPC TRC Reach phase 22 • Telewound PIA • PCVC 3.4 & 3.5 OTNInvite & Refresh • BWW Provincial Program • PMMS launch & migration to Vivify		8	4
Internal Privacy Risk Review or PSA* conducted by OTN privacy specialist	• Teleophtalmology 2.0 Mobile Camera • Telewound PSA		2	4
Other Privacy Assurance Services including consultation, by design requirements, DSAs and other Agreement language, development of artefacts, delivered to or created for the following initiatives and projects	EAPC EAPC Reach BWW Provincial Program eConsult Provincial Program PCVC Telewound BWW PMMS launch & migrate to Vivify Telepaliative Vivify Telepaliative Erie St. Clair Teleophtalmology 2.0 mobile Office 365 One Drive for Business iOS 1.3 TSM optimization & reporting Sign up 2.3.5 Customer Registration Intake Pathway Sign up Phase 2.1 CR Sign Up CASL Hub 1.9 CR Marketo redesign Webcast Center Teleophthalmology Secure Messaging Android 1.2	Directory 3.2.1 Directory 3.4 Directory 3.5 eConsult 2.2.1 eConsult 3.0.1 Consumer first 1.0 Consumer first 1.2 Consumer 1.3 VHC Marketplace Home Video wave 1 OTNInvite improvements OTN nub quick links phase 1 Office 365 TEAMS to support HVV TSM 6.0.2 Site ID (GAB) limitation CCAS reorg OTNInvite in a box Training SSO Video infrastructure refresh Practical Apps	43	30

*Privacy and Security Deliverables for Infoway funded projects include Privacy Impact Assessments (PIAs), Threat and Risk Assessments (TRAs) and Privacy and Security Architecures (PSAs). As a result of unforeseen project related delays the privacy team designed and built an internal tool/template to conduct and fast track the PSA required for the Telewound pilot in lieu of leveraging an external VOR to complete the work as it would have further delayed the launch of this initiative.. As a result all deliverables were remitted on time and approved by Infoway.

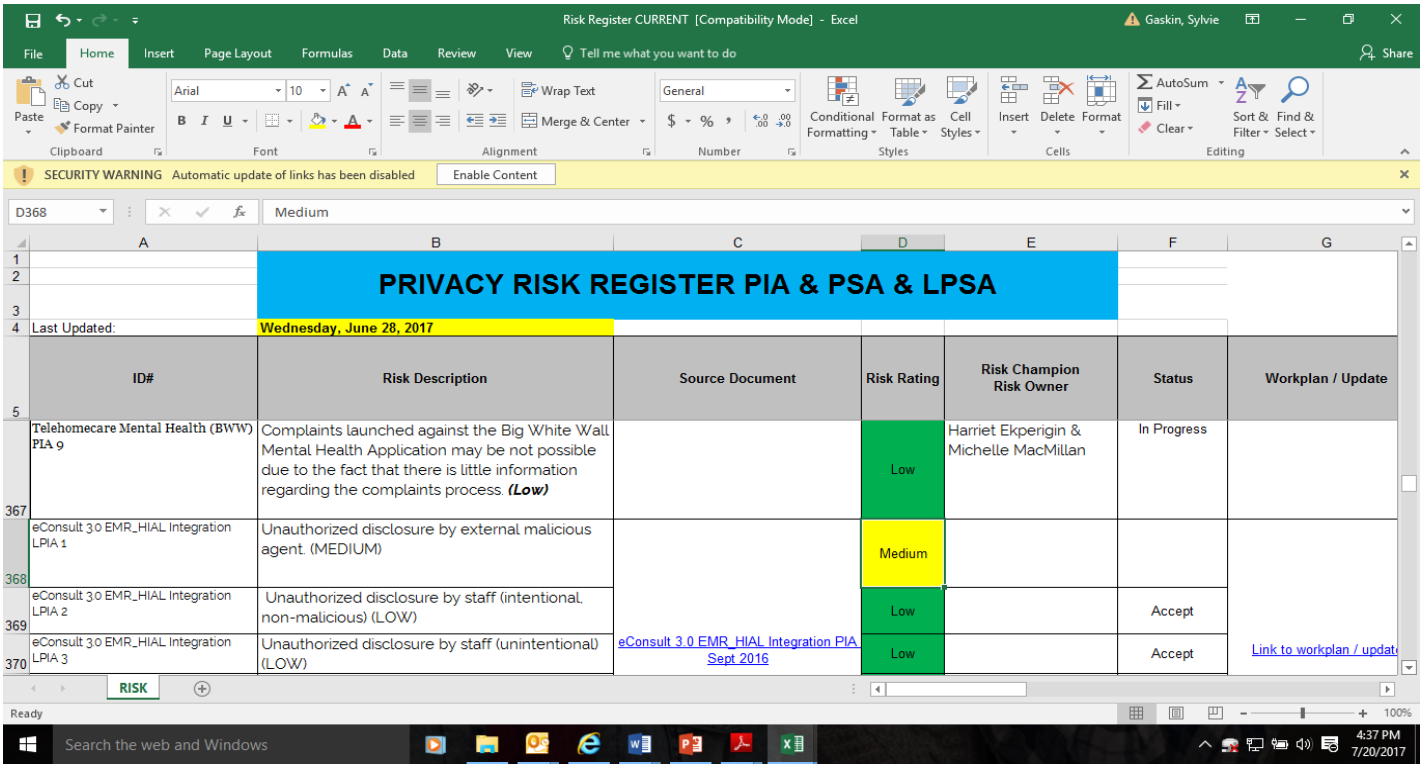
5. PRIVACY IMPACT ASSESSMENT – FINDINGS

In 2017-2018 there were 8 PIAs conducted by external VORs with internal oversight from one of the privacy specialists from OTN's privacy team, two internal privacy reviews and 1 privacy and security architecture completed internally by one of the privacy specialists. Over the course of 2017-2018 - 2 high risks, 17 medium risks and 14 low risks for a total of 33 new risks were added to the privacy risks register (see screenshot of PIA risk register below).

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. However due to competing priorities some risks (in consultation and as approved by SLT) are mitigated over a longer period of time

In FY 2017-2018, 14 high risks and 17 medium risks were closed. There are currently 3 high risks (see appendix below) and 25 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. as required under PHIPA.

Screenshot of OTN's privacy risk register



Risk Register CURRENT [Compatibility Mode] - Excel

SECURITY WARNING Automatic update of links has been disabled Enable Content

D368 Medium

PRIVACY RISK REGISTER PIA & PSA & LPSA

Last Updated: Wednesday, June 28, 2017

ID#	Risk Description	Source Document	Risk Rating	Risk Champion Risk Owner	Status	Workplan / Update
Telehomecare Mental Health (BWW) PIA 9	Complaints launched against the Big White Wall Mental Health Application may be not possible due to the fact that there is little information regarding the complaints process. ***(Low)***		Low	Harriet Ekperigin & Michelle MacMillan	In Progress	
eConsult 3.0 EMR_HIAL Integration LPIA 1	Unauthorized disclosure by external malicious agent. (MEDIUM)		Medium			
eConsult 3.0 EMR_HIAL Integration LPIA 2	Unauthorized disclosure by staff (intentional, non-malicious) (LOW)		Low		Accept	
eConsult 3.0 EMR_HIAL Integration LPIA 3	Unauthorized disclosure by staff (unintentional) (LOW)	eConsult 3.0 EMR_HIAL Integration PIA Sept 2016	Low		Accept	Link to workplan / updat

RISK

Ready

Search the web and Windows

4:37 PM 7/20/2017

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 2017-2018 the Privacy & Risk team saw a decrease in the total number of reported privacy incidents from 89 the previous year to 54 this past fiscal. The number of incidents identified as breaches also decreased from 28 in 2016/2017 to 17 in 2017/2018.

With new mandatory breach reporting requirements which came 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.

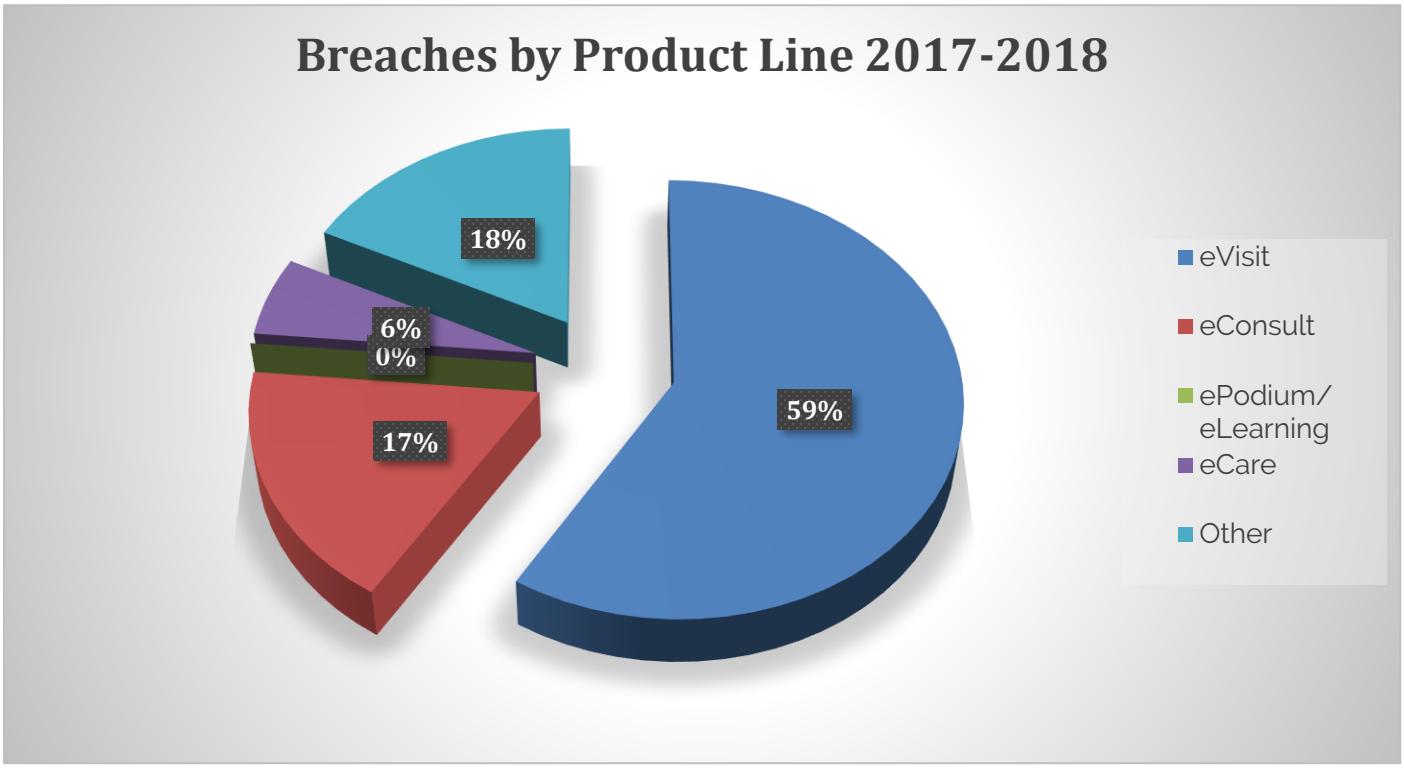
Privacy Investigations	*2012-2013*	*2013-2014*	*2014-2015*	*2015-2016*	*2016-2017*	*2017-2018*
Total # of Incidents Investigated	101	81	92	87	89	54
Total # of breaches	50	64	40	25	28	17
OTN Action	33	32	19	12	13	10
Member Action	12	30	19	12	13	7
OTN and Member Action	5	2	2	1	2	0
Breaches High Severity	0	0	0	0	0	1*
Breaches Medium Severity	4	0	1	0	1	0
Breaches Low Severity	46	64	39	25	27	16

OTN's "Contact Us" email box on the OTN.ca website was the target of a security breach.

Privacy Breaches by Product/Service

Videoconferencing and scheduling related behaviors remain the main source of privacy breaches reported. to OTN.

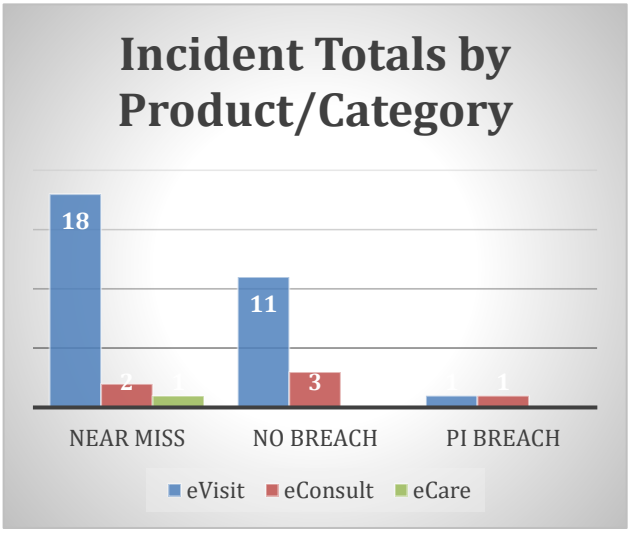
Breaches by Product/Service	*2012-2013*	*2013-2014*	*2014-2015*	*2015-2016*	*2016-2017*	*2017-2018*
Room-based videoconferencing	41	52	25	16	8	5
OTNhub	n/a	n/a	n/a	n/a	2	1
eConsult/SF	8	5	3	2	2	2
Personal Videoconferencing	0	3	4	1	2	0
TSM/Ncompass	0	0	3	4	10	6
Telehomecare	0	0	0	0	2	1
Teleophthalmology	0	1	2	0	0	0
Webcasting	1	3	3	2	1	0
Emergency Services	0	0	0	0	0	0
Learning Center	0	0	0	0	0	0
Other	n/a	n/a	n/a	n/a	1	2
Total	***50***	***64***	***40***	***25***	***28***	***17***



Videoconferencing services, room based or personal, account for over half (59%) of the breaches tracked by OTN on its network. Common root causes of videoconferencing services related breaches, are errors in account creation and delegation, practice errors by members where for example a healthcare professional may see a patient not under their care as a result of timing, auto answer functionality and/or incorrect system/site scheduling.

Following a privacy incident 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.

As noted above the highest # of incidents comes from videoconferencing services related behaviors with 18 near misses - 11 investigations which were classified as no breach and 1 Personal Information (PI) breach. The above categories encompass the following subcategories: not following best practices which had the potential of causing a PHI breach; as well errors in account creation and delegation.



The Privacy team also records and classifies non-PHI indicants which allows the team to track trends and identify improvement opportunities for both OTN employees and members.

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 the 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)

*Marketo is a marketing and email management software tool OTN is leveraging to meet its CASL obligations

CASL fines and litigation

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.

8. Trends Shaping or Informing 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 with successfully achieving its 2017-2018 key objectives:

- Marketplace/Venture Development (see operating plan section above)
- Cloud Migration (see brief overview below)
- Direct to Consumer Services (see Operating plan section above)
- Stewardship (see brief overview below)
- Data Governance & Regulatory Framework (see operating plan section above)
- Cyber Security Maturity Survey (see brief overview below)
- Privacy and the Agile Project Methodology (see brief overview below)
- From HIPPA to PHIPA (see brief overview below)
- BlockChain (see brief overview below)

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. OTN has successfully transitioned some of its operations to a cloud environment and to third party vendor cloud hosted applications. OTN is now in the planning stages of moving the OTNhub to the cloud.

OTN has several business drivers for moving the OTNhub from its current data centre to cloud web services:

1. Improved web application security
2. A need to reduce its footprint in the data centre
3. Increased availability of our services
4. Improved continuous integration and delivery pipelines resulting in faster deployment into production

From a privacy perspective a comprehensive privacy impact assessment and threat risk assessment will be conducted on this migration to ensure OTN has the right privacy and security controls as it further transitions to a cloud environment.

Stewardship

OTN is mandated to manage an open, interoperable, multi-vendor virtual care platform and to support the adoption, spread and scale, and meaningful use of virtual care to make accessing care easier for patients and more efficient for health care providers.

In accordance with this role, OTN's stewardship initiative will develop, test and make generally available a revised membership framework whereby 3rd party point-of-care videoconferencing solutions may be leveraged by eligible health care providers to provide virtual care and have their services remunerated and events counted by the province.

The Privacy Team is working with the stewardship project team to establish a framework that will include designing, testing and modifying based on lessons learned governance and operational requirements including agreements, minimum criteria for reporting, record keeping, privacy, information security, technology, training and videoconferencing etiquette and best practices.

MoHLTC Cyber Security Maturity Assessment Survey

The Ministry of Health is conducting an Ontario-wide health care setting cybersecurity maturity assessment survey. Given OTN's central role to digital health in Ontario, ongoing work supporting telemedicine and digital health across different types of care providers and vendors, the consultants secured to conduct this survey requested OTN's assistance in providing our insights prior to finalizing their survey.

Over the summer months, the Ministry conducted a cybersecurity assessment to proactively address potential security vulnerabilities in Ontario's health care system – many of them introduced or exacerbated through aging technology, broader information sharing, interoperability challenges, limited support and inconsistent security safeguards amongst health system partners. The outcome of this assessment will be to identify the current cyber posture of Ontario's digital health assets and help inform transition activities driving toward a desired future state.

OTN also completed and awaits the findings of the survey. The analysis and reporting of which are expected by the end of this calendar year.

Privacy and the Agile Project Methodology

Projects have traditionally followed a "waterfall" method ("big outcome at the end") and privacy adopted a Privacy-by-design process to manage the requirements. However, today Agile Project Methodology is dominating conversations in the project world and privacy professionals will need to adapt and adopt. Agile methods promote a cumulative build process by launching shorter "sprints" or activities within a shorter period where specific work must be completed and made ready for review. The objective is to deliver working applications frequently, from a couple of weeks to a couple of months, with a preference to the shorter time scale.

Projects typically involve organizational, product support and product feature controls. The key in managing in an agile world is to complete a fulsome review of the organizational controls such overall risk management; policies, procedures, agreements; human resource management and breach management to name a few prior to the launch of any project. By doing so, the foundation

of the project is established, and privacy specialists can focus on the key delta privacy and security requirements with each sprint cycle. It is recommended that at regular intervals, the process be reviewed and fine-tuned to adjust behaviors accordingly.

OTN is looking to utilize more Agile methods for projects in the coming year. We will update our experiences on next year's report.

From HIPAA to PHIPA

Does legal compliance translate, in full or in part, from HIPAA to PHIPA?

Numerous Canadian healthcare organizations are choosing to make use of cloud services to manage email, clinical databases, and operational systems. This is a decision that needs to be examined carefully from the perspective of privacy and security. Most cloud service providers are based in the U.S. It can be difficult to assess whether these companies are in compliance with Canadian privacy laws and standards. In the US, organizations often claim compliance with the U.S. *Health Insurance Portability and Accountability Act* (HIPAA) or with Federal Trade Commission (FTC) recommendations.

There are two kinds of cloud services offered by US companies, A) health systems, clinical and operational solutions, and B) Consumer health applications.

Many leading US cloud operations supporting clinical and operational databases have setup data centres in Canada, their compliance posture has become no different than evaluating other Canadian organizations. Therefore, the question is reduced to: ***Do health applications advertised as "HIPAA-compliant" offer some legal assurance?***

Often, the answer is no. HIPAA does not apply to technological applications as such. Rather, it governs personal health information managed by covered entities such as hospitals, physicians, pharmacies, and health insurance companies. Health applications managed by covered entities are subject to HIPAA rules. Consumer health applications managed by private businesses or independent developers are not.

What US developers of consumer health applications likely mean, when they advertise themselves as "HIPAA-compliant," is that their solution aligns with HIPAA standards, and that they are willing to sign Business Associate Agreements (BAA) with healthcare organizations. A BAA makes a service provider to a healthcare organization directly liable under HIPAA rules. Canadian healthcare organizations can obtain some legal protection by signing a BAA with a U.S.-based information service provider.

HIPAA definitely does not apply to consumer health applications, such as mobile apps and wearable devices that collect health information for an individual's use (e.g., monitoring one's exercise habits or diet), but do not share this information with a healthcare provider. Healthcare providers who wish to recommend these applications to patients should be aware that Canadians have few legal avenues to enforce their privacy rights with respect to consumer applications.

U.S cloud-based services and Canadian health organizations' compliance to them and, as a result, HIPAA compliance carry challenges but also benefits that Canadian healthcare should leverage. Measures to ensure the integrity and privacy of PHI need to be taken, including, but not limited to, HIPAA-compliant data encryption, disaster recovery, audit, management of consent, breach management, reporting, and vulnerability scanning.

BlockChain – The application of blockchain in healthcare applications

Blockchain use and understanding, is certainly on the rise. Blockchain models and tools offer a few simple yet very important benefits to healthcare. The first is the decentralization of data while offering security, audit, consent, and accountability. At a first glance, blockchain appears to offer a fit-for-purpose and fit for use solution for consumer health applications. One in which data is owned and managed by individuals themselves, a technology the offers compliance with PHIPA from Audit, Security, and consent.

The benefits of BlockChain, however don't come from these features, rather they are a result of data distribution where citizens and patients carry and pay for their own data, manage storage and distribution of data. Blockchain technology will also enable the traditional health system to engage with patients, by offering secure and private access to patients blockchain can offer patient feedback and self-reporting such as data generated from Telehomecare applications.

Blockchain is an economic and privacy and security bolstering technology.

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 in the 'Privacy Toolkit":

Privacy Impact Assessments					
3 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	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	The use of multiple sources of identity, i.e. Novel and AD, in addition to CRM.	Adhere to ISO standards on Identity Management regarding the governance, policies, processes, data, and technology.	Architecture team will work towards an integrated data model. Product team will try and align strategy with provincial identity management solution.	Enterprise identity model is in the works. Provincial integration strategy is still in very early discussion stages with eHealth Ontario. No Timing from business.	TBD not known at this time
OTN Federation PIA	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.	Information Security is working on a desired state, this has a dependency on OneID., 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	2017-2018

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