Privacy Impact Assessment Summary

Date Originally Written: Jan 26/10
Date Reviewed & Updated: August 17th 2017

Privacy Impact Assessment – Teleophthalmology 2.0

A Privacy Impact Assessment (PIA) is a risk management tool that allows the Ontario Telemedicine Network (OTN), in its role as a Health Information Network Provider under the '*Personal Health Information Protections Act, 2004*[1], 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 those recommendations detailed in the assessment.
A PIA has the benefit of generating and communicating confidence that privacy requirements are being met and risks mitigated. It can also promote fully informed policy decision-making and system design choices, ensuring privacy is considered throughout the business redesign/project redevelopment cycle. A Privacy Impact Assessment is meant to be used and expanded over the cycle of the initiative's development and implementation, to continuously identify and address risks that impact or 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 mitigated.

OTN originally completed a Privacy Impact Assessment (PIA) on the Teleophthalmology (TOP) program January 26, 2010 at the inception of the program. After six years of supporting teleophthalmology across the province, OTN recognizes the need to integrate retinal screening into chronic disease management programs.. As such, OTN has selected a new cost-effective teleophthalmology solution, Retina Labs RD Inc. (Retina), that is robust, scalable and delivered through a Software as a Service (SaaS) model hosted in Canada. Retina Labs RD Inc.. offers a product called iVision which is a web-based, secure Teleophthalmology application to support the TOP expansion.

The objective for this TOP project is to ensure that all diabetic patients in the province, regardless of their location or socio-economic situation, have access to regular diabetic retinopathy screenings. This is in line with the Ontario Government's transition to patient-centric, community-based care. Technologies like telemedicine and teleophthalmology are a key means to ensuring ubiquitous access to care while streamlining processes and reducing costs. OTN will actively promote the adoption of teleophthalmology across the province by working closely with LHINs,

[1] http://www.health.gov.on.ca/english/providers/legislation/priv_legislation/priv_legislation.html.

government agencies and healthcare organizations to build awareness and convey the benefits of the Teleophthalmology program offering.

Privcurity was selected to conduct a Privacy Impact Assessment (PIA) for the TOP program. This PIA examines the risks associated with the collection, use and disclosure of Personal Health Information (PHI) in the context of the program, as overseen by OTN and the security around the infrastructure provided by the contracted vendor, Retina Labs RD Inc.

The following is a summary of the PIA, including a brief background on Teleophthalmology, key findings & recommendations, target date for completion, and contact information for the OTN Privacy Office.

Background

The Teleophthalmology project (TOP) focuses on the provision of vision-related health care at a distance. This new initiative is based on the use of electronic means to store and transmit digitized personal health information, including images, demographic details, clinician notes, and supporting documentation. The goals of the TOP project were to:
a) improve access to retinal vision services,
b) improve the efficiency of retinal assessment, and c) reduce the burden on patients seeking treatment.

The TOP project uses a 'store and forward' model of service delivery. Clinicians at a referring site will upload digital images of a patient's retina to a central server, managed by OTN. Once loaded into this central repository, a patient's information can be accessed by vision care specialists via an internet connection. The result of the process is a diagnosis of the patient's condition, delivered to the patient by staff members at the referring site.

Key Findings/Risks & Recommendations

The PIA identified a number of privacy controls that should be enhanced to support the program. OTN has already implemented some of the recommendations and has plans in place to address others in the coming months. In the interim, temporary risk mitigation plans are in place where required.

The PIA makes the following recommendations:

#	RATING	FINDING/RISK	RECOMMENDATION	STATUS
1	High	There is a risk that data may be entered into the Retina Labs RD Inc. application, prior to gaining the patient's consent	1. The prompt to acquire patient consent prior to entering data into application should be mandatory reminder anytime the application is accessed and a patient profile is created. (NOTE: This was observed in the Staging server) 2. Privacy requires confirmation from Retina *Labs RD Inc* that the Staging server and Production server have the same information, the "consent" button operational. 3. The consent collection and timing process should be included in the Teleophthalmology Medical Administration (Training) Manual, which is being used as a training manual. 4. OTN should detail the consent collection process within the clinics	Complete Complete Complete Complete
2	High	There is a risk that PHI may be sent inadvertently to the ophthalmologist providing a second opinion from the referring TOP ophthalmologist.	1. Training Manual should include instructions on not putting any patient details into the comments section of the second opinion form. 2. Conduct random future audit/reviews to confirm that PHI is not being included in general comment field.	Complete Complete
3	High	There is a risk that PHI is included in the ocular images sent to the ophthalmologist providing the second opinion.	1. Training Manual should include instructions on not putting any patient details on ocular images. 2. Conduct random audit/review "in future" to confirm that PHI is not being included with ocular images.	Complete Complete
4	High	There is a risk that Retina Labs RD. Inc. does not have documented policies/procedures to demonstrate understanding and adherence to obligations agreed to in Service	1. Retina Labs RD Inc should create and operationalize additional privacy focused procedures. 2. Retina Labs RD Inc should post relevant documents on their website where appropriate.	Complete Complete

#	RATING	FINDING/RISK	RECOMMENDATION	STATUS
		Agreement and minimum required to adhere to privacy best practice	3. Retina Labs RD Inc. should integrate these policies/procedures as part of their overarching privacy/security program. 4. Retina Labs RD Inc. should implement criminal background screen for employees who will have access to participant site/clinic data.	Complete Complete
5	High	There is a risk associated with Retina Labs RD Inc. not providing evidence to show they meet the contractual requirement of ensuring that any of their staff with access to PHI complete privacy and security training	Retina Labs RD Inc. should document and provide formal training privacy and security training to their employees. This training should be conducted annually.	Complete
6	High	Retina Labs RD Inc. should update their breach management policy to identify when customers will be notified regarding incidents with data holdings in the care of Retina Labs	Retina Labs RD Inc. should augment their policies/procedures. The procedures must include reference that OTN to be notified upon recognition of a breach event	Complete
7	High	There is a risk that Retina Labs RD. Inc. has advised that it does not delete PHI from the iVision data base. This does not align with best practices around retention of PHI	Retina Labs RD Inc. should ensure its retention practices aligns with the obligations of the participating sites/clinics.	Complete
8	Medium	There is a risk that the OTN Training Manual outlines functionality; however, privacy obligations/messaging is not in the deck.	OTN should develop content to address appropriate privacy messaging including confidentiality of data; handling printed documentation; and identifying and reporting a breach.	Complete
9	Medium	There is a risk that the TOP solution may be making an over collection of PHI.	OTN should confirm that the data elements collected from the patient are required for interpretation of the ocular images. The Training	Complete

#	RATING	FINDING/RISK	RECOMMENDATION	STATUS
			Manual should include messaging that patient does not need to provide information if field is not mandatory.	
10	Medium	There is a risk that the wrong images will be uploaded to a patient session in iVision.	It is recommended that messaging be included in Training Manual to validate that correct images are getting added to correct patient and ensure patient details are added at time of collection of image upload which asks the user to review and confirm that the correct images are being attached to the patient session.	Complete
11	Medium	There is a risk that iVision users may not be aware of their obligations for securing the patient images which have been pre-downloaded to their location workstations - which is a collection by the provider.	1. Training Manual should include instructions on the users' responsibility for safeguarding images after they have been downloaded / printed to the authorized user's system. 2. A secure network drive should be established by clinic to act as a temporary repository prior to images being loaded to iVision 3. Information should be provided to participants on how to implement encryption	Complete Complete Complete
12	Medium	There is a risk that the iVision application sends out the one-time password and ID in an unsecured fashion.	1. A sample of the email with link tested to ensure referred physician can only see or have access to limited field 2. Training Manual should include new details and safeguarding instructions. 3. OTN should execute a Data Sharing Agreement with CPSO to enable the sharing of information among physicians	Complete Complete Complete
13	Medium	There is a risk that the letter templates from the iVision application contain too much PHI in relation to the purpose of the letter	The letter templates should be reviewed to confirm that only PHI which is necessary for reporting is included in the letter.	Complete
14	Medium	There is a risk that the Terms of Service do not cover specific TOP obligations	1. Confirmation that the Terms of Service have been updated and added to Production Server.	Complete

#	RATING	FINDING/RISK	RECOMMENDATION	STATUS
		undertaken by the HIC clinics when participating in the program	2. Confirmation that Terms of Service are available at first login by user.	Complete
15	Medium	There is a risk that the "Information Sheet" which accompanies the consent form is not aligned with the consent form signed by the patient.	Customer-facing pamphlet should be updated to ensure they align with consent form including opt-out and details on changes to the TOP service.	Q4-2018
16	Low	There is a risk that a satellite location may not be associated clearly with the clinic under whose authority it operates its practice and gains access to TOP.	All employees of participating clinics who will have access to iVision should review the relevant sections of the Training Manual and provide acknowledgement including satellite branches of participating clinics	Complete
17	Low	There is a risk that the consent form to be used by the clinics do not currently advise users that their PHI is put in a queue and available to any provider from the clinic	1. Process for general queueing should be included in patient pamphlet. 2. OTN should review clinic's consent form to confirm content.	Q4-2018 Complete
18	Low	There is a risk that PHI may be included inadvertently in the TOP ophthalmologist notification of a new pending patient interpretation	Training Manual should include information that the generic email should not include any PHI.	Complete
19	Low	If distributed, there is a risk that the TOP brochure will contain outdated information.	Customer-facing pamphlet should be updated to ensure they align with consent form including opt-out and details on changes to the TOP service.	Q4-2018
20	Low	There is a risk that the OTN Information Sheet does not include information on how to withdraw consent.	1. Training Manual should include process on how to manage a patient's withdrawal of consent. 2. Customer-facing pamphlet should be updated to ensure they align with consent form including opt-out and details on changes to the TOP service.	Complete Q4-2018

#	RATING	FINDING/RISK	RECOMMENDATION	STATUS
21	Low	There is a risk that no clear purpose statement is noted on any of the patient-facing TOP documentation.	Customer-facing pamphlet should be updated to ensure they align with consent form including opt-out and details on changes to the TOP service.	Q4-2018
22	Low	There is a risk that information about the TOP program is not currently available to patients when visiting the OTN site.	1. Privacy should review information prior to posting on its public website. 2. Customer-facing pamphlet should be updated to ensure they align with consent form including opt-out and details on changes to the TOP service.	Q4-2018 Q4-2018

Please contact the OTN Privacy Office should you have any questions:
OTN Privacy Office - Ontario Telemedicine Network
105 Moatfield Drive, Suite 1100, Toronto, ON M3B 0A2
Email: privacy@otn.ca | Tel: 416-446-4110