Privacy Impact Assessment Summary

Date Originally Written: May 24, 2013
Date Reviewed & Updated: December 2015

Privacy Impact Assessment Refresh – Identity & Access Management (IAM) ONE® ID (Phase 2)

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 completed a Privacy Impact Assessment (PIA) Refresh on its *Identity & Access Management* (IAM) ONE®ID Phase 2 service dated May 24, 2013. The PIA assessed the process by which OTN will collect data, how OTN plans to use the data, and ensure public trust that OTN handles Personal Information (PI) and access to Personal Health Information (PHI) in a responsible manner.

The following is a summary of the PIA, including a brief background on the *Identity & Access Management* (IAM) ONE®ID Phase 2 service, key findings & recommendations, status, and contact information for the OTN Privacy Office.

Background

The OTN Telemedicine Centre (TMC) portal has been developed and has launched. The portal includes key features that will allow users to access Telemedicine applications from an on-line location and will support OTN's overall goal of maximizing the use of telemedicine throughout the health care system through increased healthcare provider awareness, adoption and regular use in the support of established OTN services.

The anticipated number of users is expected to grow to 10,000 this fiscal year (2012/13) and 15,000 in the next 2 subsequent years. Simultaneously OTN is leveraging the TMC portal to support the broader roll-out of the Personal Computer Video Conferencing (PCVC) service.

In order to provision 2,000 users to the PCVC service during the fiscal year, OTN has implemented an interim trust model to ensure there are reasonable safeguards & controls in place to verify & authenticate the identity and authority of these users. OTN is now working to integrate with eHealth Ontario's ONE® ID IAM services for face-to-face identity validation, registration and enrollment of OTN users within Ontario at a medium level of assurance (AL2) commencing in the summer/fall of 2013.

[1] Ontario Ministry of Health and Long-term Care. "Health Information Protection Act, 2004." http://www.health.gov.on.ca/english/providers/legislation/priv_legislation/priv_legislation.html.

Care. Connected.

Key Findings/Risks & Recommendations

The PIA identified privacy controls that should be enhanced to support the IAM ONE® ID Phase 2 program. OTN is in the midst of developing a risk management plan and collaborating with eHealth Ontario, as required, to address the risks. The PIA noted the following risks and recommendations:

#	RATING	FINDING/RISK	RECOMMENDATION(S)	STATUS
1	High	The governance model and business owner for the OTN IAM service has not been made explicit – therefore there is a risk of lack of clear accountability for the IAM service. [carry over from Phase1]	OTN should ensure that there is a business owner identified and accountable for OTN Identity and Access Management Services.[Carry over from Phase 1]	Complete
2	High	OTN and eHealth Ontario have not entered into a formal agreement for the integration of eHealth Ontario ONE® ID Services and OTN IAM Services which clearly sets out the accountability for each organization therefore there is a risk that OTN will not have a clear understanding of the risks it is accepting in partnering with eHealth Ontario.	OTN should ensure that the draft agreement with eHealth Ontario has been thoroughly reviewed, that the content is clearly understood, vetted through legal counsel and signed off prior to services being made available to OTN users.	Complete
3	High	OTN and eHealth Ontario have not developed a governance structure for the shared IAM service delivery model which will provide the necessary direction for the shared service.	OTN and eHealth Ontario should develop and implement a governance structure for the shared service.	Complete
4	High	In accepting the terms and conditions of the OTN/eHealth Ontario Services Agreement OTN is accepting the responsibility for ensuring OTN end-users are meeting certain conditions (including	OTN should develop an end-user click through agreement that will ensure that accountability for meeting eHealth Ontario terms and conditions are passed to the end-user. This should also set out consequences of non-compliance.	Complete

#	RATING	FINDING/RISK	RECOMMENDATION(S)	STATUS
		training of end-users on privacy and security). There is a risk that end-users will not be aware of, and therefore not comply with, these requirements.		
5	Medium	There is a risk that if OTN assumes the role of LRA that individuals assigned to the role may not understand their obligations as the organizational infrastructure to support this has not yet been established.	OTN should determine which positions within the organization will be eligible to assume this additional role, must ensure that there are criteria for selecting who is equipped to assume this role, must revise position descriptions to ensure that LRA's understand their roles, and must ensure that these individuals receive training in identity validation.	Complete
6	High	There is a risk that users will not be aware of the purpose for which OTN is collecting PI and therefore, OTN will not be compliant with PIPEDA (OTN will be considered to be engaging in commercial activity when charging for services.)	It is recommended that OTN inform users of the purposes for which the PI is being collected and the fact that it will be disclosed to eHealth Ontario in providing the services.	Complete
7	High	There is a risk that OTN users will not be able to consent to the collection, use and disclosure of their PHI because they are not aware of the purposes for which PI is being collected, used, or disclosed.	When informing users of the purposes for which PI is being collected, used or disclosed, OTN should also include that the individual has the right to withdraw consent at any time and should provide them with instructions on how to do so. This information should be provided before the user is asked to provide any PI.	Complete
8	High	There is a risk that eHealth Ontario may not have the necessary authority to collect PI as the PI is not being used for the 'Agency's information infrastructure' but for the use of OTN's services.	It is recommended that OTN and eHealth Ontario determine whether PI is required in the provision of services to OTN and if so, ensure that both eHealth Ontario and OTN are satisfied that eHealth Ontario has the necessary authority to collect, use and disclose it as required.	Complete

#	RATING	FINDING/RISK	RECOMMENDATION(S)	STATUS
9	Low	There is a risk that OTN does not have a schedule for the retention of any personal information that is collected but no longer used for purposes of identification of former TMC/PCVC users. [Carry over from Phase 1]	OTN should update its Data Retention Schedule to include any personal information collected and used in the identification and validation process. [Carry over from Phase 1]	Complete
10	Medium	There is a risk that OTN's retention and sanitization policy and procedure may not reflect current methods for sanitization. [Carry over from Phase 1]	OTN should review its Data Retention and Sanitization policy to ensure that it remains current and should schedule the next review date. [Carry over from Phase 1]	Complete
11	Medium	There is a risk that OTN does not have a written process for, and therefore does not consistently apply, the process for de-registration of TMC and PCVC users. [Carry over from Phase 1]	OTN should ensure that there is a written process for de-registering individuals who no longer need access to OTN applications or explicitly request that any personal information be removed from OTN databases. [Carry over from Phase1]	Complete
12	High	There is a risk that end-users will not let OTN know that they no longer need their ONE® ID account and therefore OTN will not be able to let eHealth Ontario know in a timely fashion that a user should be de-registered.	It is recommended that OTN seek to revise the existing language in the eHealth Service Agreement to require that OTN end-users are obligated to inform eHealth Ontario that the user no longer requires access to the system and eHealth Ontario will then de-register the user. (Provided that this does not interfere with a process that OTN may arrange for de-registering users to TSM.) It should also require that eHealth Ontario run regular audits of the utilization of accounts and de-register users who have not met certain user parameters (e.g. a user has not logged into the system within a certain time period.)	Complete
13	Medium	There is a risk that OTN will fail to accurately verify the identity of existing users as the LRAs may not be	OTN should ensure that each identified LRA receives thorough training on the tools and process of validating identity and	Complete

#	RATING	FINDING/RISK	RECOMMENDATION(S)	STATUS
		properly trained to do so.	recording information correctly.	
14	Medium	There is a risk that TMC Users will fail to update their identity related data used by OTN. [Carry over from Phase 1]	It is recommended that end-users be required to notify eHealth Ontario at earliest opportunity if their identity related critical business information changes and that users are made aware of this requirement through click through agreement, policy/procedure and training/communication means.	Complete
15	High	There is a risk that data quality/accuracy may be impacted due to the manual nature of the OTN user registration process. (	It is recommended that OTN develop a mechanism for data quality control and implement the same (e.g. including but not limited to a process for how to deal with 'duplicate errors' or conflicts').	Complete
16	Medium	There is a risk OTN has not finalized a TRA on the new ONE® ID integration process.	It is recommended that OTN finalize a TRA on the new ONE® ID integration with a scope that includes people, process and technology. It should also consider the existing outstanding risks from the ONE® ID TRA summary which has been provided by eHealth Ontario.	Complete
17	High	There is a risk of lack of clarity around the help-desk support arrangements for when users are unable to log into the system (e.g. Have forgotten their password) – will users contact OTN or eHealth Ontario? If users contact OTN, how will OTN confirm the identity of the caller?	It is recommended that OTN confirm the operational process and tools for user support and ensure that if OTN will be providing support that there is a standard procedure for validating the identity of those calling for new passwords.	Complete
18	Medium	There is a risk that there is a lack of administrative safeguards (policies, procedures) that have been developed and implemented to provide clarity and direction on the IAM related processes.	It is recommended that OTN develop the required IAM specific policies and procedures to ensure that all involved understand how to a) validate identity b) manage identity related PI c) manage any issues that arise in the process.	Complete

#	RATING	FINDING/RISK	RECOMMENDATION(S)	STATUS
19	Medium	There is a risk that OTN is not prepared for a large scale breach involving any personal information used for identity purposes. [carry over from Phase 1]	It is recommended that OTN review its enterprise security and privacy breach management processes to ensure scale.	Complete
20	Medium	There is a one-time risk of PI (DOB) being transferred from OTN to eHealth Ontario as the means for the sharing this information with eHealth Ontario is unclear.	It is recommended that OTN and eHealth Ontario confirm the means by which PI can be shared electronically using a secure mechanism and that the infrastructure to do so is established (technical, process and people).	Complete
21	Medium	There is a risk of PI (user ID and Password) being compromised during the process of the LRA providing a password as the mechanism and process for obtaining the one time password and providing it to the potential registrant is not clear.	It is recommended that OTN and eHealth Ontario confirm the means by which the user ID and password is generated, how it comes to be known by the LRA and how it is provided to the potential registrant at the face-to-face meeting.	Complete
22	High	There is a risk that users or potential users of OTN's services will not be made aware of the purposes for which OTN is using PI.	It is recommended that OTN update the 'Privacy Notice on the Protection of Personal Information' to state what information is being collected and that it is being used for purposes of registration, validation of and authentication of identity for authorization of access to OTN data assets. It should also state that this information is being disclosed to eHealth Ontario for the same purpose.	Complete

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

Care. Connected.