Privacy Impact Assessment Refresh Summary

Date Originally Written: 24 January 2013
Date Reviewed & Updated: 15 September 2014

Privacy Impact Assessment – Telemedicine Centre / Identity & Access Management (Refresh)

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 it's 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) on its *Telemedicine Centre / Identity & Access Management (Re-fresh)* service dated January 24, 2013. The PIA assesses the process by which OTN will collect the data, how OTN plans to use the data, and ensure public trust that OTN handles PHI in a responsible manner.

The following is a summary of the PIA, including a brief background on the *Telemedicine Centre / Identity & Access Management* service, key findings & recommendations, status, and contact information for the OTN Privacy Office.

Background

TMC is a Secure-Socket Layer (SSL) portal that is to serve as a gateway to OTN's service offerings. IAM is intended to be part of a framework for the

[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.

identification of individuals, the verification of those identities, the assignment of assurance levels in connection with the provision of credentials, and eventual authorization to access specific OTN services. Collectively, TMC and IAM will provide the front-end interface to OTN's clinical, educational, and administrative services.

It's important to note that during the completion of the PIA; OTN finalized the manual interim identity validation processes and this was reviewed and evaluated. These processes will support the roll-out of IAM and will be used to further augment existing OTN processes.

Key Findings/Risks & Recommendations

The PIA identified some privacy controls that should be enhanced to support the IAM program. OTN has put temporary risk mitigation plans in place where required and has plans in place to address others in the coming months. The PIA noted the following recommendations:

#	RATING	FINDING/RISK	RECOMMENDATION(S)	STATUS
1	High	The governance model and business owner for the IAM service has not been made explicit – therefore there is a risk of lack of clear accountability for the IAM service.	OTN should ensure that there is a business owner identified and accountable for OTN Identity and Access Management Services.	Complete
2	Medium	OTN has not established a policy and associated procedures for Identity and Access Management therefore there is a risk that employees, affiliates and users may not have the clarity that they may require in performing their functions in support of IAM.	OTN should review the existing policies, procedures and guidelines to determine whether revisions to the documents should be made to accommodate the IAM process (for example, aspects of the 'Privacy Guidelines for Caller Identity & Authority Verification' might be more suitable for a policy and could be adapted to accommodate verification of callers more generally) and should ensure that its employees, affiliates (Telemedicine Coordinators), and users are aware of the obligations that they may have under such policy and procedure.	In Progress

#	RATING	FINDING/RISK	RECOMMENDATION(S)	STATUS
3	Low	There is a risk that existing users may not be aware that their personal information will be collected and used for identification and validation purposes.	It is recommended that OTN notify existing users of the introduction of the new system and that their business information will be used in the identification and validation process.	Complete
4	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	OTN should update its Data Retention Schedule to include any personal information collected and used in the identification and validation process.	Complete
5	Low	There is a risk that OTN's retention and sanitization policy and procedure may not reflect current methods for sanitization	OTN should review its Data Retention and Sanitization policy to ensure that it remains current and should schedule the next review date.	Accept
6	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.	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.	Complete
7	Medium	There is a risk that OTN will fail to accurately verify the identity of existing users and therefore expose OTN to the possibility of an	OTN should implement rigorous administrative mechanisms which will ensure that there is appropriate oversight for the validation process and for the manual process of entering the validated information into the Novel IAM system to ensure that	Complete

#	RATING	FINDING/RISK	RECOMMENDATION(S)	STATUS
		unauthorized user having access to personal health information.	data is accurate when entered. OTN should establish a formal policy and procedure for verifying the identity of individuals when information is being collected from them over the telephone. A standard script should be created for the Customer Support Team to ensure that this occurs in a consistent fashion.	
8	Medium	There is a risk that TMC Users will fail to update their identity related data used by OTN.	It is recommended that either a) the TMC User Agreement be updated to include the requirement to notify OTN at earliest opportunity if their identity related critical business information changes or b) that users are made aware of this requirement through policy/procedure and training/communication means.	Complete
9	Medium	There is a risk that data quality/accuracy may be impacted due to the manual nature of the migration 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').	In Progress
10	Medium	There is a risk that systems administrators can bypass interface controls and implement backdoor processes that could cause a risk that may not be detected in a timely manner.	It is recommended that OTN implement a process or technology to control and limit access to backend application. This can be implemented through a 'security' change request requiring business approval. In addition, access to backend tools could be designed to require a specific one-time password, and a two-person authentication.	Complete
11	Low	There is a risk that using an internally developed method 'stripping of identifiers' may leave reversible	It is recommended that OTN implement a commercial grade anonymization tool to ensure that data in the warehouse is not reversible and will not allow for identification or re-identification.	Complete

#	RATING	FINDING/RISK	RECOMMENDATION(S)	STATUS
		identifiers and hence data may be identifiable.		
12	High	There is a risk that OTN allows connections through expired certificates as users (internal or external) may have the habit of accepting invalid or expired certificates and hence causing a significant threat.	OTN should expedite the remediation of expired certificates.	Completed; All Certificates Current & Up-to-date
13	Medium	There is a risk that OTN is not prepared for a large scale breach involving any personal information used for identity purposes.	It is recommended that OTN review its enterprise security and privacy breach management processes to ensure scale.	In Progress
14	Low	There is a risk that provider individuals that are members of OTN delegate their responsibilities to administrative assistants and there isn't the capability to currently identify 'delegates' in the system.	It is recommended that OTN consider making system modifications to allow for the appointment of 'delegates.'	Complete
15	Medium	There is a risk associated with the lack of face-to-face validation for grandfathered users.	In the absence of the implementation of a face-to-face identification and validation process that OTN increase its capacity for monitoring systems/alerts for indication of potential unauthorized/inappropriate use and be prepared to contain any	Complete

#	RATING	FINDING/RISK	RECOMMENDATION(S)	STATUS
			potential breaches of security. Further, it is recommended that OTN consider decreasing the length of time for automatic 'deactivation' from the current 1 year time frame to a more constrained time frame until such time that a face-to-face identification process can be established.	

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