Privacy Impact Assessment Summary

Date Originally Written: 1 June 2012
Date Reviewed & Updated: January 2016

Privacy Impact Assessment – Telemedicine Centre / IAM

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) on its Telemedicine Centre / Identity & Access Management service dated May 30, 2012. 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, target date for completion, 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 identification of individuals, the verification of those identities, the assignment of assurance levels in connection with the provision of credentials, and eventual

[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.

authorization to access specific OTN services. Collectively, TMC and IAM will provide the front-end interface to OTN's clinical, educational, and administrative services.

Key Findings/Risks & Recommendations

The PIA identified some privacy controls that should be enhanced to support the program. Although no risks were identified in the PIA document, a number of recommendations were noted to augment or mature OTN's privacy program. The PIA noted the following recommendations:

RECOMMENDATION	STATUS
If documentation is to be submitted by users, integrate such documentation into OTN document retention practices (i.e. fix retention period, determine where they will be stored and how they will be securely destroyed).	Completed
Integrate 3rd parties into OTN's breach notification protocols.	Completed
Prepare summary of the proposed IAM program, including a description of the requirements for the program and a description of how the program will or does meet those needs. Create a separate description of the IAM service for publication, with a particular emphasis on the identity verification aspects.	Completed
With respect to identity verification: • Establish and document processes employed. • Develop audit measures and controls • Minimize amount of data required, including copies of documentation for users with higher level credentials • To the extent that OTN relies on 3rd parties to verify identities for authentication & subsequent authorization to use OTN services, define OTN and 3rd party roles and responsibilities for identify verification • To the extent that the disclosure of information may occur in the verification of identities establish and document conditions and requirements associated with the disclosure of personal information • Visually verify identification documents for users with higher-level credentials	Completed

RECOMMENDATION	STATUS
Ensure security issues identified in the TRA are adequately addressed.	In Progress
Create a separate description of the IAM service for publication, with a particular emphasis on the identity verification aspects.	Completed
To ensure consistency between the site privacy statement and OTN organizational privacy statement move to one statement for OTN services and use it on the site or revise the proposed TMC privacy statement to make it more specific to the TMC-IAM service offerings	Completed
For access request management purposes, create a system to document the processing of authentication requests in connection with the IAM service	Completed
If documentation is to be submitted by users integrate such documentation into OTN's retention practices (i.e. fix retention period, determine where they will be stored and how they will be securely destroyed). user submitted documentation into OTN document retention practices.	Completed

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