Privacy Impact Assessment Summary

Date Originally Written: March 2014
Date Reviewed & Updated: January 2016

Privacy Impact Assessment – eConsult 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) refresh on its eConsult Phase 1 service dated March 2014**.** 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 refresh, including a brief background on the eConsult, key findings & recommendations, and contact information for the OTN Privacy Office.

Background

The eConsult project is comprised of a web-based application, supporting business processes and an underlying *store and forward* technology infrastructure. The eConsult application will enable healthcare professionals to more efficiently exchange patient health information with one another, to electronically request advice from one another, to refer patients to one other, and to better coordinate the overall care of their patients.

Ontario's privacy legislation requires OTN to conduct a Privacy Impact Assessment (PIA) of the eConsult/ project. In May 2013, Ontario Telemedicine Network engaged GRA Consultants Inc. to complete a PIA of the first phase of the project (the "Prototype Demo" phase). This PIA Refresh builds on that prior PIA, and additionally assesses the changes and new functionality that will be implemented for Phase 1.

Key Findings/Risks & Recommendations

The PIA identified some privacy controls that should be enhanced to support the eConsult service. OTN has already completed some of the recommendations and has plans in place to address others in the coming months. The PIA makes the following recommendations:

#	RATING	FINDING/RISK	RECOMMENDATION(S)	STATUS
1	Low/Medium	**Ad Hoc Delegate Account Management Processes** For the eConsult Pilot, OTN is largely relying on ad hoc manual procedures for managing delegate accounts (e.g. registration, provisioning, associating with practitioners etc.). This introduces a risk that delegates may be inappropriately granted or denied access to patient information.	Processes for managing delegate user accounts should be integrated with standard OTN IAM processes.	Completed eConsult users will be migrated to the OTNhub by December 2014 and as such the account management processes will be integrated with the standard IAM processes
2	Low	**Uncertainty Regarding Applicability of Bill 78 to OTN** If Bill 78 passes, and if it is determined that OTN is subject to EPHIPA, OTN may not be prepared to take on additional privacy responsibilities related to maintaining an EHR, such as managing patient consent, managing public accountability, and reporting to the IPC	OTN should monitor the progress of Bill 78 in the Ontario Legislature OTN should seek a legal opinion upon passage of Bill 78 and its associated regulations, such as to determine its applicability to OTN, if any.	Accept ePHIPA is still in second reading
3	Medium	**Mixing of Patient Identifiers from Different Sources in the eConsult Database** The eConsult database maintains a patient index containing demographic data (including Health Numbers) for use by eConsult and by other OTN applications. Each of these applications is able to search the patient index and add	OTN should consider partitioning the patient index into different views corresponding to each application that uses the index	In Progress This recommendation will be implemented in the next release of the eConsult application

		new patients. However it is not clear whether: • OTN has the authority to create and maintain a patient index, or has obtained appropriate approvals, • the requirements for creating and maintaining a patient index have been subject to appropriate privacy and security review, or • the patient index has appropriate controls to separate stakeholders based on purpose. There is risk of unauthorized access to PHI if access to the patient index is not appropriately controlled and limited	OTN should articulate appropriate business requirements, including P&S requirements, for the creation and operation of a shared patient index	In Progress At the time this PIA was conducted not all business, privacy and security requirements had been adequately documented.OTN is in the process of augmenting its documentation and will ensure recommendations are addressed for the next eConsult release – only patients associated with a user can be accessed by that user; however the the eConsult database recommendation will be addressed in the next eConsult release
4	Medium	**Extraneous Patient Information in Image and Video Files** New eConsult functionality allows images and videos to be uploaded and attached to eConsultation. This introduces the risk of accidentally including extraneous patient information into the files, such as a patient's face or voice	OTN's eConsult end-user training/awareness program should provide guidelines to providers on limiting the collection of patient information during the creation and processing of the image and video files that are uploaded to eConsult. For example, a patient's face should not be included in an image or video unless it is pertinent to the consultation request; similarly, the audio track which is recorded with a video should be muted or deleted unless relevant to the consultation.	Completed This information has been added to the click-thru user agreement
5	Medium-High	**Inability to Delete PHI from the eConsult Database** • PHI cannot be	OTN should ensure that PHI can be irretrievably purged from the eConsult database	In Progress OTN will address this

		permanently deleted from the eConsult database. Records can be flagged as 'REMOVED' but physically no record can currently be permanently be deleted.	A schedule for purging of PHI from the eConsult database should be developed and implemented in accordance with statutory requirements, Member Agreements, and OTN policies	recommendation in the next release
				In Progress OTN will address this recommendation in the next release –at a minimum the data will be retained for the duration of the pilot – this information was added to the click-thru agreement
			If it is not possible to permanently remove PHI from the eConsult database, then OTN should ensure that – in alignment with OTN policy – the information can be securely de-identified	In Progress OTN will address this recommendation in the next release
6	Medium	**Ad hoc Privacy Reporting Processes** It is not clear whether OTN has the capability to produce appropriate privacy reports from the eConsult log files: • As a HINP, OTN is required to provide to HICs upon request, an electronic record of all accesses and transfers of personal health information associated with the custodian • OTN's Logging and Monitoring Policy also requires that audit logs capture every addition, modification, and deletion to PHI, as well as the identity of every user who accesses PHI. Although not explicitly stated in	OTN should ensure that appropriate privacy reports can be generated from eConsult audit logs as required to meet OTN's obligations as a HINP, and to meet the reporting requirements implied by OTN's Logging and Monitoring Policy	Completed

		the policy, OTN must also be able to appropriate produce reports from the log files on demand		
7	Low-Medium	**Inadequate Labelling of Printed Reports** • eConsultations exported to PDF files contain a privacy disclaimer on the first page of the document but not on subsequent pages, and the disclaimer in its current form is too verbose to reasonably be included on every page • PDF document pages are not numbered for completeness • Failure to appropriately label documents containing PHI could lead to careless handling of the documents, potentially resulting in a privacy breach	OTN should ensure that the privacy disclaimer appears in the footer of every page of exported PDF files and not just the first page	Completed
			OTN should shorten the privacy disclaimer so that it can reasonably fit on each page of the PDF file	Completed
			OTN should ensure that pages in the PDF files are numbered for completeness (e.g. page 1 of 5) in the page footers	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