Privacy Statement of Risk Summary

Date Originally Written: November 12, 2019
Date Reviewed & Updated: November 13, 2019

Privacy Summary – Partner Video Project

A Privacy Impact Assessment (PIA) is a risk management tool that allows the Ontario Telemedicine Network (OTN) 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.

In certain circumstances, OTN will complete a Statement of Risk (SR) that applies a similar methodology in assessment as the PIA to address identified risks and recommend appropriate mitigation to promote a fully informed policy decision-making and system design choices, ensuring privacy is considered throughout the business redesign/project redevelopment cycle. A SR 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 Statement of Risk for the Partner Video Project on Nov 12, 2019. The following is a summary of the SR, including a brief background, key findings & recommendations, target date for completion, and contact information for the OTN Privacy Office.

Background

The Partner Video Project (PVP) is a limited enrollment initiative through which health care organizations and providers can trial and help inform the recommended provincial approach that could enable broader use of non-OTN technology in Ontario, while not inadvertently fragmenting or decreasing access to virtual care. This includes requirements for technology standards, , accountability agreements, data/reporting, representation on the directory and enabling supports that may be needed (e.g. procurement, privacy and security). Partners are defined as publicly funded organizations such as hospitals as well as private practice physicians (who themselves are a legal entity). Through the Project:

- Providers are remunerated for care delivered via non-OTN video visit technology that meet minimum standards and guidelines;
- Partners will participate in focused demonstration projects to inform development of a provincial framework for the opening of the virtual care marketplace; may include testing and supporting workflows for patient host site interactions; and
- Partner video will enable as many providers and organizations as possible to easily use virtual care to expand access to care.

The PVP will present options and recommendations, for Ministry of Health (MoH) consideration, to implement designed to accelerate the adoption and utilization of virtual care technologies, within the context of a coordinated provincial approach.

Under MoH direction, OTN will leverage its recent experience with several proofs of concept to launch the PVP in a phased approach. The goals of enabling partners to use other video solutions are to:

- increase use of virtual care solutions across the health care sector, with a focus on video to the home;
- provide the opportunity to use Hospital Information System/Electronic Medical Record (EMR)-integrated video;
- maintain and where possible equitable access to care province wide;
- meet regional and hospital-level needs;
- effectively deliver integrated, high-quality care to patients;
- enhance both the patient and provider experience overall; and,
- create efficiencies in how care is delivered with a focus on reducing hallway medicine

Partners are required to transmit virtual care activity data directly to OTN. The designated party (partner or vendor) is responsible for implementing its respective privacy and security protocols until data is uploaded to the Partner Portal (SharePoint) within OTN infrastructure after which OTN becomes accountable. This Statement of Risk (SR) represents the point when OTN becomes accountable upon receipt of the evaluation data (demarcation point). OTN will act as an Agent for the Health Information Custodians (HICs) or partner under PHIPA. PHIPA defines an Agent to include any person who is authorized by a HIC to perform services or activities on the Custodian's behalf and for the purposes of the Custodian. The Agent may have access to PHI, as directed by the HIC to perform a specified function which for the PVP is the evaluation of the PVP. PHIPA permits Custodians to provide PHI to their Agents only if the Custodian is permitted to collect, use, disclose, retain or dispose of the information. The partner is responsible to collect consent from the patient to advise on the sharing of their personal health information (PHI) with OTN. The consent must reference that PHI or de-identified data will be sent to OTN for evaluation purposes. If the patient refuses to provide consent, the member will de-identify the PHI and send to OTN. The MoH Transfer Payment Agreement (TPA) guides OTN's involvement and role with the project

The project is currently in 2 distinct phases with additional functionality to be addressed at a later date:

- Phase 1 involved member submission, via the Partner Portal, of a "csv" file that reflects the visit results and the sharing of participating physician registration information, including an executed PoC Agreement, completed OHIP telemedicine billing forms (where the physician hadn't already been registered to bill OHIP for telemedicine encounters) and information required to publish the physicians identity, where agreed by the partner, onto the OTN Directory – these exchanges were via email.
- Phase 2 which is now in progress enables partners to submit all physician registration information through the Partner Portal with exception of the PoC Agreement which continues to be executed via email.
- The future deliverables, listed in the Appendix, will require a privacy review once details are available and before implementation.

Each project has distinct parts: Onboarding, Patient Visit/Transmission and Data Collection

The Process

As part of the PVP activation process, knowledge resources are shared within the Partner Portal. One such resource is a Partner Video Readiness Self-Assessment which includes a range of questions and considerations partners are recommended to address prior to participation in the PoC

- questions cover governance and accountability, videoconferencing best practices and etiquette, patient information and recordkeeping, data and reporting, technology, privacy and security, and training and awareness. Once the partner confirms that they are comfortable with having met PoC participation requirements and executes the PoC Agreement, an activation process is initiated to enable physician registration and data sharing. In order to access the Partner Portal, partners are required to designate two or more site admins and specify which will have access to the data submission section. Once physician registration is complete and processed, where required (some physicians already have OHIP telemedicine billing in place), billing may ensure.

Provincial standards for vendor technologies are being drafted and will be implemented as part of the Partner Video framework. Vendors will be required to attest to meeting a set of minimum mandatory requirements in order for their customers (Partner Video partners) to bill OHIP for consultation performed with the vendor's technology. On the 6th business day of following month, the partner uploads the PHI and masked data to their portal. At OTN, a Process Automation Service is scheduled to connect each transmitted data file to the data warehouse (MARS) by extracting the data from the Partner Portal and then routing it to MARS. All PHI is stripped, and the data is converted to the required Key Performance Indicators (KPIs): (mileage, length of visit). The KPIs will be made available to OTN staff and the MOH as part of OTN's monthly reporting.

Only OTN's Data Governance team, who are under a confidentiality agreement and undergo annual privacy training, will have access to the PHI and non-PHI data as well as to the calculated metrics in the Data Warehouse. All data in the warehouse is encrypted during transition and at rest using industry best practice cryptography standards. Access to the data sharing portal is provisioned for individual users only. Sharing of credentials is not permitted. All access to upload and download data is logged for auditing purposes. Audit logs include the username of users designated to access data, date and time of the access and the artefact being accessed.

.

Key Findings/Risks & Recommendations

The privacy analysis of the initiative identified ***6 risks*** all of which were classified as low. OTN's PIA ***policy recommends that all high/medium risks be mitigated*** to an acceptable level prior to a project going live. As such the following recommendations, should be implemented prior to or in concert with this project's launch. The recommendations should reduce the risk ratings ***from High to Medium*** and from ***Medium to Low.*** The identified-Low risks should be mitigated within a reasonable time as determined by the Privacy Team. Risk rating used to assess the risk of each identified gap are available upon demand.

The PIA makes the following recommendations:

#	Risk Level	Finding/Risk	Recommendation (s)	Status	Responsible Party
1	L	At partner login, PI may be stored outside of Canada during the authentication process for O365, which is contrary to OTN Cloud Policy. Data also becomes subject to foreign jurisdictions.	• Obtained exception of OTN Cloud Policy to allow PI/PHI to be stored outside of Canada. • Amending the agreement between OTN and the participants to authorize storage and transmission of PI for authentication outside of Canada. • Amending the OTNHub Terms of Service to authorize storage and transmission of PI for authentication outside of Canada • Adding message bars on screens within SharePoint that PI may need to be sent outside of Canada based on Microsoft policy; including the caution that users should not include PI/PHI within files it uploads to SharePoint.	**COMPLETE**	Privacy; Contract/legal Corporate IT
2	L	More PHI is sent than required for project. OTN receives more PHI than required.	Audit transmission of member/technology provider to ensure only required information is sent; if more, data is securely disposed of and member informed of error.	Ongoing	OTN Data team
3	L	De-identification of PHI for non-consented patients is performed incorrectly by partner resulting in unconsented PHI being sent to OTN.	Audit transmission of member/technology provider to ensure only required information is sent; if more, data is securely disposed of and member informed of error.	Ongoing	OTN Data team
4	L	Unauthorized access to Data Warehouse might occur. PHI may	Audit capabilities available within Data Warehouse to monitor access; OTN has	Ongoing	OTN Data team

		be accessed inappropriately.	implemented annual privacy training and confidentiality agreement acknowledgement as administrative measures to prevent unauthorized accessed.		
5	L	During evaluation stage, data is not properly masked to prevent re-identification. PHI can be accessed without authorization.	Audit capabilities available within Data Warehouse to monitor access; OTN has implemented annual privacy training and confidentiality agreement acknowledgement as administrative measures to prevent unauthorized accessed. OTN will develop a Data Deidentification protocol and an accompanying Policy to provide privacy guidance on process.	Pending	OTN Data team OTN Privacy
6	L	The retention being contemplated may not comply with PHIPA. The current retention period is set at 7 years for the data in the SharePoint portal and 15 years for the MARS database.	OTN will undertake a review to determine if there is an appropriate rationale for the length of the retention period.	Pending	OTN Privacy

Please contact the OTN Privacy Office should you have any questions:

OTN Privacy Office - Ontario Telemedicine Network
438 University Avenue, Suite 200, Toronto, ON M5G 2K8
Email: privacy@otn.ca | Tel: 416-446-4110