



Privacy Impact Assessment Summary

Care Coordination: Patient Access Network (PAN) Scheduling (Limited Release)

Date Originally Written: October 27, 2021

Date Reviewed and Updated: October 27, 2021

A Privacy Impact Assessment (PIA) is a risk management tool that allows Ontario Health (OH), in its role as a health information network provider under the ‘*Personal Health Information Protection 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.

OH publishes PIA summaries to ensure transparency with its members, users, the public, and those individuals who may be the subject of the personal and/or personal health information collected, used, disclosed, retained or disposed of in relation to OH’s products or services. OH also publishes these summaries to ensure compliance with the requirements for health information network providers under Ontario Regulation 329/04 (s. 6(3)). Without the express written consent of OH, the summaries or the content therein may not be copied, used, or redistributed outside of the purposes identified above.

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 OH and/or its partners.

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.



The following is a summary of the PIA, including a brief background on the Care Coordination: Patient Access Network (PAN) Scheduling project (eVisit 4.9.1), key findings and recommendations, target date for completion, and contact information for the OH Privacy Office. The PIA for the eVisit 4.9.1 release was conducted by an external consultant and completed in June 2021.

Background

In late 2020, OH began a project (eVisit 4.9.1) to improve the workflow for scheduling Patient Access Network (PAN) sites, which host patients for Video Visits. These hosting services are critical for patients who may experience barriers to their participation in Direct to Patient Video Visits, including a lack of high-speed internet access or a requirement for nursing support during a Video Visit.

Initially, the eVisit 4.9.1 project contained two key components: 1) a new workflow for consultants and their schedulers on the OTNhub, and 2) the distribution of Outlook licenses to select PAN sites to enable integration of PAN site availability and scheduling data with the new OTNhub workflow. The PIA conducted on the eVisit 4.9.1 project identified 16 total risks, including 5 high and 7 medium risks, with most high and medium risks related to the Outlook component of the project. As a result, the Outlook component was de-scoped from the eVisit 4.9.1 release and may be contemplated separately in the future.

With the Outlook component de-scoped, only 4 risks remained that were applicable to the OTNhub component of the project, including 1 high risk and 3 medium risks. Any findings, observations and recommendations in this report are based on a review of project documentation at the time of the assessment. The following table is a summary of the risks and recommendations and is shown in risk severity order.

Key Findings/Risks & Recommendations

With the Outlook component of the project removed, the privacy analysis of the initiative identified 4 risks. OH's PIA policy recommends that all high and 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 definitions used to assess the risk of each identified gap are available upon demand.

The PIA makes the following risks and recommendations:

#	RATING	FINDING/RISK	RECOMMENDATION/MITIGATION	STATUS
1	High	When a scheduler is booking a patient host site in OTNhub, the patient address should be identified as optional. The address field does not appear to be labelled as optional in the latest screenshot viewed. A previous rendition in the requirements document reviewed did identify the address field to be optional.	A pop up/just in time notice should appear when the address field is hovered over to explain that this information is only required if the scheduler would like the patient's address to be populated into the patient letter.	Completed
2	Medium	Documented policies under review by the Ontario IPC must be finalized with an implementation/operationalization plan. Legacy Ontario Telemedicine Network (OTN) policies and procedures are being rolled into the OH policies yet to be confirmed.	The OH suite of privacy policies and procedures will apply to eVisit 4.9.1. Where the OH framework differs from what exists for the legacy OTN, the internal privacy team must assure the eVisit 4.9 projects are in alignment with these components.	Mitigation measures in place reduce residual risk to low. Mitigation measures include legacy business unit privacy policies and procedures which remain in effect until new policies and procedures are harmonized



#	RATING	FINDING/RISK	RECOMMENDATION/MITIGATION	STATUS
				and privacy training for all staff.
3	Medium	Privacy event audit logging has not been confirmed or documented by the project team for eVisit 4.9.1. Note that event logging requirements have been provided for event scheduling activity in OTNhub, but must also incorporate MS O365 accounts (including view-only activity of PHI contained in Outlook files).	Privacy event audit logging has not been confirmed or documented by the project team for eVisit 4.9.1. Note that event logging requirements have been provided for event scheduling activity in OTNhub, but must also incorporate MS O365 accounts (including view-only activity of PHI contained in Outlook files).	Completed for in scope elements (i.e., OTNhub workflow).
4	Medium	Retention rules have not been established for scheduling related data that will be contained in the OTNhub database and in Outlook e-mail files. Retention practices are yet to be approved by Chief Privacy Officer and Archivist of Ontario.	eVisit 4.9.1 scheduling records must be included in the retention schedule so Outlook records (.OST files) are not retained indefinitely (cancelled events may warrant a longer retention timeframe than completed events that are already recorded/maintained in the source system NCompass/TSM).	Mitigation measures in place reduce residual risk to low. Mitigation measures include retention of scheduling data (with plans to accommodate long-term retention of data in alignment with existing regulatory requirements



#	RATING	FINDING/RISK	RECOMMENDATION/MITIGATION	STATUS
				and guidance from oversight bodies) until the new retention schedule is finalized and privacy training for all staff.

Please contact the OH Privacy Office should you have any questions:
Email: OH-OTN_privacy@ontariohealth.ca