Ontario Health
OTN

Privacy Impact Assessment and Statement of Risk Summary

Secure Messaging (iOS, Android, OTNhub) (Full PIA and Delta PIA)

Secure Messaging (Additional OTNhub Features and Provincial Roll-Out Preparation) (Statements of Risk)

Date Originally Written: September 2018
Date Reviewed and Updated: February 1, 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 (PHIPA)'*[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

[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.

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. OH 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.

The following is a summary of the PIA, including a brief background on the Secure Messaging project, key findings & recommendations, target date for completion, and contact information for the OH Privacy Office.

Background

OH owns and operates the OTNhub, a virtual care platform that provides access to thousands of users across several core services, including Video Visit and eConsult. Feedback from the field indicated demand for an unstructured messaging service for ad hoc collaboration, shorter questions, and care coordination. In response to this demand, OH entered into a signed agreement with a limited number of OH Members to launch a Proof of Concept (POC) initiative to provide Secure Messaging functionality to those OH Members.

The first phase of the Secure Messaging POC initiative provided Secure Messaging functionality, via the OTNConnect App, to a limited number of OH Members using iOS devices. A full PIA was conducted on this project phase in September 2018. Subsequent project phases enabled Secure Messaging functionality for select OH Members using the OTNhub (i.e., desktop browser endpoint) and Android devices, via the OTNConnect App. To identify risks associated with the deployment of Secure Messaging functionality to these new endpoints, OH completed a delta PIA for the Android and OTNhub phases of the POC pilot in March 2019.

After completion of the delta PIA for the Secure Messaging OTNhub and Android releases, additional scope was added for the OTNhub endpoint. As such, a privacy Statement of Risk (SoR) was conducted to assess the additional scope in September 2019. A final privacy Statement of Risk was conducted in March 2020 to ensure readiness for an anticipated provincial roll-out of Secure Messaging functionality.

Ontario Health
OTN

Key Findings/Risks & Recommendations

The four assessments described above identified a total of 15 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 ratings used to assess the risk of each identified gap are available upon demand.

The assessments made the following risks and recommendations:

Secure Messagion iOS PIA and Secure Messaging Android and OTNhub Delta PIA

#	RATING	FINDING/RISK	RECOMMENDATION/MITIGATION	STATUS
1	Medium	End users may not remember the terms and conditions that they are required to meet under the relevant agreement(s) which may lead to unauthorized collection, use and disclosure of sensitive information including Personal Information and Personal Health Information (PI/PHI).	A short disclaimer should be presented to the end user each time they login to the OTNhub informing the end users of the purpose for which they are to use Secure Messaging. The disclaimer should inform end users that any collection, use, disclosure or handling of PI/PHI is subject to PHIPA, including any PHI where a patient has withdrawn consent. The language should also warn users against copying, pasting and/or exporting data that may lead to unauthorized collection, use, disclosure and handling of PI/PHI.	In Progress

Ontario Health
OTN

#	RATING	FINDING/RISK	RECOMMENDATION/MITIGATION	STATUS
2	Medium	There is a risk of unauthorized access, use, disclosure and handling of sensitive information, including PI/PHI, in the event the mobile device is lost or stolen if the end user fails to secure the device. Without enabling user authentication security features, a thief may be able to access to the contents of the phone including the secure messages.	OH should require end users to enable authentication security features on their phone (i.e. PIN or password and locking after a period of inactivity), as well as prohibit mobile devices that have been jail broken from connecting to OH services).	Completed
3	Medium	There is a risk that OH is in non-compliance with its Health Information Network Provider (HINP) requirements under s.6(3) of O.Reg.329/04, as the current *OTNhub Terms of Service for Member Organizations, June 2018*, does not provide an accurate and up-to-date plain language description of the Secure Messaging function which is part of the OTNhub service.	Prior to rolling out the Secure Messaging function as a service and after the POC, OH should amend *OTNhub's Terms of Service for Member Organizations, June 2018* and update the description of services to include a description of the Secure Messaging function, as well as the purpose for which members and users may use the messaging feature.	Completed

#	RATING	FINDING/RISK	RECOMMENDATION/MITIGATION	STATUS
4	Medium	Without providing a publicly available description of the Secure Messaging function, applicable policies, guidelines and a description of safeguards, there is a risk that OH is in non-compliance with its HINP requirements under s.6(3) of O.Reg.329/04.	Prior to rolling out the Secure Messaging function as a service and after the POC, OH should update its website to include a description of the Secure Messaging function and include relevant policies and guidelines, as well as a high-level description of safeguards.	Completed. A Services and Safeguards document has been finalized and distributed to pilot participants and will be made available on otn.ca should the initative transition from pilot to full roll-out.
5	Medium	Without readily available and accurate audit logs, there is a risk of delays in responding to requests by participating sites for audit logs in the event of a privacy and/or security breach, which may delay containment and investigation efforts.	OH should develop queries and reports that automatically capture the required fields as described under s.6(3) paragraph 4 of O.Reg. 329/04, to ensure that this information is readily available upon request. Efforts should also be made to log the HIC of the PHI in an accurate manner (as opposed to deriving the HIC from the user name). A documented procedure must exist to ensure OH only transmits sensitive audit logs that may contain PHI to authorized individuals from member sites.	In Progress

#	RATING	FINDING/RISK	RECOMMENDATION/MITIGATION	STATUS
6	Medium	There is a risk that OH is in non-compliance with its HINP requirements under s. 6(3) of O.Reg. 329/04 due to missing provisions in the agreement between OH and the third-party vendor that require the vendor to comply with the restrictions and conditions necessary to allow OH to comply with its HINP requirements.	OH to amend its agreement with the vendor to include provisions that require the third-party vendor to comply with the restrictions and conditions necessary to allow OH to comply with its HINP requirements.	Completed
7	Medium	The OH *OTNhub User Agreement, June 2018*, does not include a description of the Secure Messaging function. Without including a description of the Secure Messaging function in the agreement, there is a risk of ambiguity with respect to the roles and responsibilities of OH and users.	Prior to rolling out the Secure Messaging function as a service and after the POC, OH should update the its *OTNhub User Agreement, June 2018*, to include a description of the Secure Messaging function and to make it clear that the Secure Messaging function is part of the existing OTNhub services. The requirements in the agreement are general requirements that will apply for Secure Messaging as well.	Completed
8	Medium	A documented offboarding procedural document is not in place for OH's clients	OH to draft and develop offboarding procedures that address offboarding and revocation of credentials for its clients using OH services. This	Completed

#	RATING	FINDING/RISK	RECOMMENDATION/MITIGATION	STATUS
		using OH services. The absence of documented offboarding procedures may lead to ambiguity with clients as well as potential delays in containing privacy and/or security breaches involving OH services where end user access needs to be removed. Improper offboarding may also lead to a higher likelihood of unauthorized access and use when user accounts remain active in error, resulting in a privacy and/or security breach, and a higher likelihood of procedural breakdown when relevant staff leave due to improper knowledge transfer.	documented procedure should be shared with the clients using OH services to ensure that they are aware of the proper procedures, and for knowledge transfer purposes.	
9	Medium	Two (2) different sets of addresses for sending the *Privacy Complaint Form* to OH may lead to confusion with respect to form submission. In the event that one of	OH to review and update all public facing forms with the correct mailing address.	Completed

#	RATING	FINDING/RISK	RECOMMENDATION/MITIGATION	STATUS
		the addresses is no longer valid, there is a risk that Privacy Complaint Forms containing sensitive information could be sent to the wrong address.		
10.	Medium	In the event that the POC/Pilot is extended beyond the limited number of OH Members already participating, this PIA may not suffice due to the limited scope. Without a PIA to assess Secure Messaging services beyond current pilot participants, there is a greater risk of unauthorized handling of PHI and non – compliance with OH's legislative, contractual and administrative requirements.	Should the POC/Pilot of the Secure Messaging service be extended to a larger audience beyond current pilot participants, a PIA must be undertaken to assess any changes and to ensure all safeguards are in place including the mitigation of risks and compliance with OH's legislative, contractual and privacy policy requirements. This PIA must also assess whether processes/mechanisms are in place to ensure that OH can meet the requirements of its clients including (but not limited to) meeting retention requirements and responding to individual access requests in a timely manner.	Completed. Privacy Statement of Risk Completed February 2020.
11.	Low	The hyperlink in OH's *OTNhub User Agreement, June 2018* that directs users to *OH's Privacy Statement* appears to be out-of-	OH should update the hyperlink in OH's *OTNhub User Agreement, June 2018* with the hyperlink provided in the iOS Privacy Notice. In updating the hyperlink in the OTNHub User Agreement, June	In Progress

#	RATING	FINDING/RISK	RECOMMENDATION/MITIGATION	STATUS
		date and only describes the collection of PI in the context of OH's website. In contrast, the hyperlink provided in the *iOS Privacy Notice* contains a comprehensive description of services offered by OH. Without consistency in *OH's Privacy Statement*, there is a risk of confusion and lack of clarity around the services offered by OH including OH's practices around the collection, use and disclosure of PI/PHI.	2018, OH should not limit the Privacy Notice to iOS as the Secure Messaging Service will also be deployed for Android devices and OTNhub App Browser. The Privacy Notice should be inclusive for iOS, Android and OTNhub App browser users.	
12.	Low	*OH's Privacy Statement* does not include a description of the Secure Messaging function as part of existing OTNhub services. Without a description of the Secure Messaging function in *OH's Privacy Statement,* there is a lack of transparency around OH's handling of PI/PHI with respect to	Prior to rolling out the Secure Messaging function as a service and after the POC, OH should update its *Privacy Statement* to include secure messaging as a function that is being offered as part of the existing OTNhub services.	Completed

#	RATING	FINDING/RISK	RECOMMENDATION/MITIGATION	STATUS
		the Secure Messaging service.		

Secure Messagion OTNhub SoR and Secure Messaging Full Provincial Roll-Out SoR

#	RATING	RISK/FINDING	RECOMMENDATION/MITIGATION	STATUS
1	Medium	Although mitigation plans are in progress, there is a risk that the 5 outstanding medium risks from prior assessments may not be mitigated prior to full roll-out of the Secure Messaging solution.	Mitigate all medium risks in accordance with documented action plans prior to the Secure Messaging full roll-out.	In Progress
2	Low	Permitting users to export, save or print attachments creates a risk of unauthorized disclosure of PHI by users and/or members. OH's existing agreements do not clearly articulate that users/members become responsible for the appropriate management of exported/transferred PHI, creating a risk for OH in the event of a privacy breach.	OH should consider adding additional language to the OTNhub User Agreement under *User Obligations* (section 2c), clearly indicating the following: • Any content exported or transferred from OH applications becomes the responsibility of the user (and/or the associated member (HIC)) who exported/transferred it. • Users must ensure that any PHI exported or transferred from OH applications is managed in accordance with their organizations' privacy policies and PHIPA.	Completed

#	RATING	RISK/FINDING	RECOMMENDATION/MITIGATION	STATUS
			• Users must follow their organization's privacy breach management procedures in the event exported/transferred PHI is lost, stolen, or otherwise used or disclosed without authority. The OH Privacy Office should also be notified in such instances. OH should consider adding the language suggested above to the OTNhub Member Terms of Service under section E, *Personal Health Information*. OH should consider adding the language suggested above to a pop-up banner or message that appears when information is saved, exported, or printed from any application in the OTNhub.	
3	Low	By retaining Secure Messaging attachments indefinitely, there is a risk that OH may retain PHI and other confidential information for longer than is reasonably required to fulfil the intended purpose.	OH should consider implementing a defined retention period for Secure Messaging attachments. The retention period should be long enough to allow health information custodians to fully comply with their record keeping requirements (i.e., 10-15 years), but stop short of indefinite retention. Attachments may also be deleted at the express request of the relevant health information custodian(s).	In Progress. Retention Schedule is undergoing review and revisions as part of integration with Ontario Health.

Ontario Health
OTN

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

438 University Avenue, Suite 200, Toronto, ON M5G 2K8
Tel: 416-446-4110 Fax: 416-446-4139 www.otn.ca