Privacy Impact Assessment Summary

Ontario Virtual Care Clinic (OVCC) - Novari Health

Date Reviewed and Updated: October 15, 2020
Date of OVCC Privacy Impact Assessment (PIA): July 10, 2020
Related PIAs for eVisit Primary Care (eVPC) Originally Written:

August 2017	PIA Phase 1 (GRA Consultants)
January 2018	PIA Phase 2 Refresh #1 (GRA)
April 2018	PIA Phase 3 Refresh #2 (GRA)
March 2019	Internal Privacy Review (OH Privacy)
June 2020	Statement of Risk (OH Privacy)

Privacy Summary – Ontario Virtual Care Centre – Novari Health

A Privacy Impact Assessment (PIA) is a risk management tool that allows the Ontario Health (OTN Business Unit) ("OH") 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 information, personal health information and deidentified information (collectively "data") 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, under *'Personal Health Information Protection Act, 2004'*[1]for Health Information Network Providers (HINP) under Ontario Regulation 329/04 (s. 6(3)), as an Electronic Service Provider (eSP) (General, O Reg 329/04, s. 6(1)) and as an Agent. OH does not permit the summaries or the content therein to be copied, used, or redistributed outside of the purposes identified above, without the express written consent of OH.

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 PIA 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

[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 potential to impact the confidentiality, integrity and accessibility of data held/handled by OH and/or its partners.

OH completed the Privacy Impact Assessment (PIA) for OVCC and the accompanying eVPC PIAs as detailed in table on previous page. The PIAs assess the process by which OH will collect the data, plans to use the data and the management of third parties used in the solution to ensure public trust that OH handles PHI in a responsible manner. OH has adopted a "low" risk tolerance level, meaning that low and very low risks will not be immediately actioned, but will be actioned at an agreed upon time to ensure they do not develop to be higher risks. All high and medium risks are to be mitigated prior to a product or service launch or obtain an exception as detailed in the OH PIA Policy. The PIAs assess the process by which the project will collect the data (personal information (PI)/personal health information (PHI) /deidentified/aggregated), how it plans to use the data and ensure public trust that the project handles the data in a responsible manner.

Background

This document provides a summary of the PIA conducted by OH's Privacy team. The assessments conducted on eVPC involving Novari Health act as background but also as a foundation as Novari uses the same platform to deliver OVCC. OH launched a procurement with qualified eVPC suppliers for a Virtual Wait-Room. Novari Health was selected as the solution provider with a Master Agreement (MA) and Statement of Work (SoW) governing the delivery of the solution. The OVCC is to support Ontarians who do not have a family doctor or who cannot access their family doctor during the pandemic. OVCC is a free-to-the-patient, secure online service developed with technology provided by Novari Health (Novari) eVisit solution. It is for non-urgent, non-COVID-19 primary care issues where a physician can be accessed via secure videoconference or audio. The partners include the Ontario Medical Association (OMA), OntarioMD (OMD), funding from Canada Health Infoway (CHI) and support from the Government of Ontario Ministry of Health (MoH). The OVCC solution is built on the same platform (same entry point) for the eVPC and their private client portal. **This PIA for OVCC reflects information provided up to June 30, 2020.**

The OVCC solution can be accessed in two methods:

1. Patients can access OVCC directly from the website, *"seethedoctor.ca".* The site information has been promoted through various channels. From there, they are directed to the Novari portal, "*virtualcarenow.ca"*, agree to the Consent, EULA and Novari Privacy statement and are directed to the next available on-call physician.
2. The program also connects through Telehealth Ontario (THO). THO, when determining that a primary care physician is required for a non-COVID-19 inquiry, can refer the patient to the *seethedoctor.ca* site. The patient will follow the same sign-up procedures as previously discussed. The intent of the relationship with THO is for OVCC to assist THO to manage the excessively high call volumes during the pandemic.

The OVCC will enable THO to refer patients to a virtual website to see an on-call physician support the project. The project has been developed to help THO manage the excessively high call volumes during the COVID-19 pandemic. This project will build capacity for THO to focus on their

COVID-19 protocol and assessments, while redirecting non-COVID related primary care calls to an on-call physician supporting the OVCC. To summarize the conclusions:

- Health Information Custodians (HICs) remain in custody or under control of Personal Health Information (PHI) available in OVCC.
- OH remains accountable and has demonstrated its recognition of accountability for PHI/Personal Information (PI) and deidentified data.
- OH complies with the requirements of a Health Information Network Provider (HINP) and Agent under Personal Health Information Protection Act (PHIPA).
- OH and Novari have identified the purposes for which the information is being collected.
- Consent is obtained from patients through the solution during the registration process in an online consent form. Novari has the ability to track consent.
- Novari is a Service Provider to OH under a Statement of Work (SoW).

Legislative authority

Personal Health Information Protection Act, 2004 (PHIPA)

Compliance with PHIPA is a shared accountability between the participating physicians, Novari, the partners and OH. OH has multiple roles under PHIPA such as a Health Information Network Provider, eService Provider and Agent. Novari will solely act as an eSP throughout the project, under the direction of OH. The PHIPA regulation defines the requirements that the various participants must meet. The requirements are meant to provide the HICs to which the HINP and eSP provides its services with assurance that the HINP and eSPs are appropriately managing the data. OH and its service partners have agreed to meet these requirements in its agreements with the sending and receiving facilities and have developed privacy and security safeguards to support in meeting these requirements.

Freedom of Information and Protection of Privacy Act (FIPPA)

On April 1, 2020, OTN was transferred into Ontario Health through the Connecting Care Act, 2019; as such, all rights, and obligations of OTN transferred to Ontario Health. Ontario Health is designated as a FIPPA institution as per the FIPPA Regulations and as such is subject to FIPPA. The purposes of FIPPA are:

1. to provide a right of access to information under the control of institutions in accordance with the principles that,
    - information should be available to the public,
    - necessary exemptions from the right of access should be limited and specific,
    - decisions on the disclosure of information should be reviewed independently of the institution controlling the information; and
2. to protect the privacy of individuals with respect to personal information about themselves held by institutions and to provide individuals with a right of access to that information.

All accompanying documentation related to the initiative may be subject to a Freedom of Information request.

Other: *Canadian Anti-Spam Law* (CASL)

The solution utilizes alerts and messages by way of email/text. The current interpretation of the law does not allow a health information exemption so the program must meet the obligations as mandated by CASL.

Key findings of the PIAs

OH considers two key factors when determining the severity of privacy risks:

i. The potential *impact* to OH and its members, users or patients should the identified risk result in a privacy breach or non-compliance with applicable legislation and/or best practices.
ii. The *likelihood* of a breach or instance of non-compliance occurring if safeguards/mitigation measures are not implemented.

The goal of privacy risk management is to ensure privacy risks remain within acceptable limits. Higher risk ratings indicate priority areas for risk mitigation. The more vulnerable OH is to the risk, the higher the impact will be should the event occur. If risk responses including controls and safeguards are not in place and operating as designed, then the likelihood of an event increases. The PIA identified **23 privacy risks**, of which **9** were rated as **Medium** and the rest as **Low**. OH's PIA policy recommends that all **high and medium risks be mitigated** to an acceptable level prior to a project/initiative going live. 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. OH has already closed some of the recommendations to an acceptable level and will continue to monitor the risk level to ensure it remains within the acceptable level as determined by the policy. The following table lists the MEDIUM open risks and provides the current status as of September 30, 2020:

Ontario Health

#	Risk Level	Item	Risk	Mitigation plan (Recommendations)	Status
1	M	Novari Authentication takes place in United States.	The data stored in Azure AD B2C for each account is: • A randomly generated unique id • The user's s email address and password (stored hashed) • The URL of the Novari web application being logged into This is contrary to OH's Cloud Computing Services Use and Procurement policy.	1. Privacy must obtain an exemption from the policy directive to allow for data to be stored outside of Canada.	Exemption obtained. CLOSED
2	M	Patient records maintained within OVCC are the only source of the visit (some physicians may record information in their personal Electronic Medical Record (EMR) but not mandated). Physician can print by creating PDF/excel or download and add to a patient file it must create for each visit.	There is a risk that the OVCC could be deemed to be an EMR with the accompanying obligations that are currently not being met.	2. OMD's Hospital Report Manager (HRM) should be implemented. 3. This would make OVCC a secondary source of PHI and reduce OH's retention obligation for PHI. 4. Physicians must be reminded to download encounter reports from every patient visit to their office files. 5. Physicians must establish files in their offices for each patient. 6. Another option is to apply for and make OVCC an EMR.	PENDING
3	M	There is a need to coordinate the management of	There is a risk that the lack of coordination may result in unnecessary escalation of events.	7. For openness and transparency, a coordinated approach to	PENDING

		complaints, compliments, questions, inquiries and breaches among the partners when dealing with patients. OntarioMD (OMD) manages the physician relationship.		complaints, questions, inquiries and breaches among the partners.	
4	M	Physicians are asked to perform a visual authentication/ identification of OHIP.	There is a risk that the patient could be wrongly identified due a number of factors such as poor connection, card problems.	8. Investigate adding automated verification of OHIP card with link to Ministry database to reduce identification risk. Investigate other Identity Access Management (IAM) vendors.	PENDING
5	M	The collection of physician PI is managed by Ontario Medical Association (OMA)/OMD and sent to Novari to establish a profile on OVCC. The information is not fully visible by patients when look at physician information.	There is a risk that patients may not be able to make an access request of their PHI held by physician if physician creates a patient file. This would be in contravention to PHIPA access rules.	9. Add physician information to OVCC physician profile which can be accessed by patient to allow them to access PHI. (see Recommendation # 5)	PENDING
6	M	Physicians do not have access to previous visits within OVCC if a patient has selected to choose OVCC for a second time or more.	There is a risk that physician may be making health care decisions without a set of full information.	10. Allow for physician to access previous visits of patient.	PENDING
7	M	OMD has been provisioned with administrative access.	There is a risk that OMD staff may inadvertently access patient information without the “need-to-know” basis. In privacy,	11. Novari’s audit capabilities mean they can track where what users have	PENDING

		OMD requires access to the queue list in order to manage the wait room; however they also have the ability to click on patient and view the full profile. OMD only requires access to Patients Waiting, Estimated Wait Time and Members on Call.	if an individual has the ability to, implies they may eventually access PHI/PI.	accessed and including patient records, any type of user action against a record (add, update, delete, etc.). OH should request an audit report from Novari to determine if there has been unauthorized access. 12. OMD's ability to view patient information and access full patient profile should be eliminated.	
8	M	OVCC is reliant on patient and physicians to connect electronically; this does introduce the possibility of bandwidth and connectivity issues. If a connection is broken, physicians will tend to continue visit through their office telephone line. If after hours and physician is not in office, they could use personal home phone or cell.	There is a risk that during a connectivity issue, details of a visit could be lost and force the participants to choose alternate methods to continue visit. A telephone line outside of solution is not as secure. Use of personal lines is contrary to Terms of Use and inherently not secure.	13. The project should develop plan to address connectivity, so patients' health visit is not compromised. 14. Investigate what happens to information collected if the connection is broken prior to completion. 15. Add to OVCC material the potential of connectivity issues and what would happen. Add to Frequently Asked Questions (FAQ)? Consent? Terms?	PENDING
9	M	OVCC allows for patient/caregiver use.	There is a risk that the information around caregivers and dependents is not properly recorded.	16. Novari should add a section where caregiver/dependent information are separate from the patient of visit	PENDING

				can be added. Also to consider is the separation of parent/guardian from dependent should the situation warrant. 17. Privacy to address differing retention issues adult vs. dependent timelines.	

Please contact the Privacy Office should you have any questions:

Email: privacy@otn.ca | Tel: 416-446-4110 / 1-855-654-0888 / TTY: 1-855-368-6889