Privacy Impact Assessment Summary

Remote Care Management (formerly Telehomecare): Vivify Go+ for iOS and Android App

Date Originally Written: October 2019
Date Reviewed and Updated: January 7, 2022

Privacy Summary – Vivify Go+

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

Ontario Health 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 Ontario Health's products or services. Ontario Health also publishes these summaries to ensure compliance with the requirements for health information network providers under Ontario Regulation 329/04 (s. 6(3)). Ontario Health 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 Ontario Health.

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 Ontario Health and/or its partners. Ontario Health 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.

Ontario Health completed a Privacy Impact Assessment (PIA) on Vivify Go+ dated *July 30th, 2019*. The PIA assesses the process by which Ontario Health will collect the data, how

Ontario Health plans to use the data and ensure public trust that Ontario Health handles PHI in a responsible manner.

The following is a summary of the PIA, including a brief background on *Vivify Go+*, key findings & recommendations, target date for completion, and contact information for the Ontario Health Privacy Office.

Background

Ontario Health brings virtual care innovation to the healthcare system so that the people of Ontario can get the care they need when and where they need it most: at home, in their community or in hospital. For more than a decade, Ontario Health has increased access to health care and education across the province with one of the world's most extensive telemedicine networks. Working with its many partners and leveraging its unique knowledge of health care and digital technology, Ontario Health addresses challenges by introducing and spreading new ways of delivering care that benefit patients, care providers and the healthcare system.

In 2017, Ontario Health engaged Vivify Health to develop, host and administer the Remote Care Management (RCM) program (previously referred to as Telehomecare). The Vivify solution that is currently deployed has 2 modalities of access for patients:

- Fully managed kits consisting of an Android tablet and health monitoring devices such as blood pressure cuffs, pulse oximeters and/or weight scales. These Bluetooth enabled devices are paired with the tablet by Vivify Health allowing the app on the tablet to automatically obtain the device readings and upload them to Vivify. The entire kit is pre-configured by Vivify and shipped to the patient as part of enrolment; and
- A BYOD (Bring Your Own Device) solution where the patient uses their own health monitoring devices and uses a mobile device app to manually enter their device readings and upload them to Vivify.

Vivify released a mobile app (Vivify GO+ v2.0 for iOS and Android) as a new feature of their service on May 30, 2019. These apps replaced the original BYOD Go+ web based app which was decommissioned in July 2020. The mobile app provides features to patients wanting to use their own health monitoring devices including:

- Bluetooth connectivity to a list of Vivify-supported health monitoring devices (currently not enabled);
- Biometric Self Trending on patient's mobile device;
- Secure Messaging between the patient and their Patient Care Team;
- Video visits between the patient and their Patient Care Team; and

- Educational Videos and Health Tips.

Ontario Health would like to make these apps available for patients with their own monitoring devices attending delivery sites who are using remote management services from Vivify. Using these apps will provide these patients capabilities similar to the Fully Managed Kit solution.

The patient's care team consisting of their health care providers will in turn have the ability to view and communicate with their patient through the existing web-based Care Team Portal (out-of-scope).

Key Findings/Risks & Recommendations

The privacy analysis of the initiative identified 8 risks, 2 classified as high and 6 mediums. Ontario Health'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 risks and recommendations:

#	Risk Level	Finding/Risk	Recommendation (s)	Status
1	High	Exhibit "A" Services, Deliverables and Timelines and Schedule C of the Master Service Agreement between OTN and Vivify Health Canada Inc. does not include a description of the +GO iOS and Android app as well as the now decommissioned +GO Web App services that will be offered by Vivify. Without a clear description of the +GO iOS and Android app, as well as the now decommissioned +GO Web App, it is not clear that these services are	Ontario Health and Vivify to update the Master Service Agreement with a description of +GO iOS and Android app, as well as the now decommissioned +GO Web App, services that will be provided to Ontario Health by Vivify. Amendment B to Vivify Contract April 3, 2019, mitigates and retires this risk.	Completed

		subject to the terms and conditions in the Master Service Agreement.		
2	High	The Master Service Agreement does not explicitly include notification requirements between Ontario Health and Vivify in the event that there is a privacy and/or security breach. Without notification requirements pertaining to privacy and security breaches between Ontario Health and Vivify, there is a risk that privacy and security breaches may go unreported. In addition, this may also lead to ambiguity with respect to whom to contact and within what time frame notification must be given. Without relevant terms and conditions in the Master Service Agreement containment efforts may also be delayed leading to a greater impact on the privacy and/or security breach.	Ontario Health and Vivify to update the Master Service Agreement with notification requirements including who to contact and the time frame (24 hrs) of notification in the event that either party detects a privacy and/or security breach pertaining to +GO iOS and Android app as well as the now decommissioned +GO Web App. Amendment C to Vivify Contract Nov 5, 2019, mitigates and retires this risk.	Completed
3	Medium	Without a finalized EULA for +GO iOS and Android app, as well as the now decommissioned +GO Web App, there is a risk of lack of accountability on the patient end user with respect to the +GO services. In addition, the current EULA for use of the Vivify Solution with your own device (mobile phone, tablet/iPad,	It is recommended that OH and Vivify finalize the EULA for +GO iOS and Android app as well as the now decommissioned +GO Web App prior to go-live to ensure that accountabilities of the end user patients are clear. In finalizing the EULA, consideration should be given to the following:	Completed

		laptop/MacBook, desktop) does not include terms and conditions around suspension and termination of services which may be required for containment efforts in the event of a privacy and/or security breach or notification requirements in the event that the end user suspects a privacy and/or security breach. Furthermore, the current EULA does not include provisions that requires the end user not to compromise or tamper with the +GO app, as well as the now decommissioned +GO Web App, in a manner that may lead to privacy and security breach. Lastly, under section 2, second bullet, the EULA states, "I understand that all communication with my Host Organization will be either by phone or through the check-in platform." It is not clear if this "check-in platform" includes +GO app, as well as the now decommissioned +GO Web App, services as the "check-in platform" is not defined in the EULA. This may cause confusion for patient's reading this EULA as it is not explicitly clear what this "check-in platform" includes.	- Adding terms and conditions that allows for suspension and/or termination of services in the event of privacy and/or security breach; - Notification requirements in the event of suspected privacy and/or security breach; - Provisions that requires end users to maintain the integrity of the GO iOS and Android, as well as the now decommissioned +GO Web App; and - Ensuring the EULA is in plain language and up to date.	
4	Medium	The Consent Script Checklist does not include any guidance on what to do	Ontario Health to update the Consent Script Checklist with guidance for	Completed

		when a patient wishes to no longer participate in the +GO iOS and Android app, as well as the now decommissioned +GO Web App, or BYOD and Fully Managed Kits. Although the duration of the program is only 6 months, it is possible that a patient may wish to no longer participate during this 6-month time period. Without clearly documented guidance on what to do when a patient wishes to withdraw from the program, there a risk of procedural breakdown and ambiguity which may lead to unauthorized collection, use and disclosure of PHI.	Remote Care Monitoring clinicians, on what to do, who to contact, and what to say to the patient when a patient wishes to no longer participate in the +GO iOS and Android app as well as the now decommissioned +GO Web App. There is ability in the app to have a patient unenroll, can use a messaging feature that they want to be unenrolled. Care team changes their status; the app will still reside on their phone; stop receiving push reminders, no longer able to see screens and input data.	
5	Medium	Privacy & Remote Care Monitoring, 2018/19 privacy training for the patient's care team members does not reflect the use of iOS and Android +GO apps as well as the now decommissioned +GO Web App by patients. Without updating the training, the patient's care team may not be able to assist patients when they have questions around the use of the app or need assistance.	Privacy & Remote Care Monitoring, 2018/19 privacy training to be updated so that the patient's care team are educated on the new iOS and Android +GO apps, as well as the now decommissioned +GO Web App, used by their patients in order to be able to assist their patients and correctly direct them to the proper contact when needed.	Completed
6	Medium	Ontario Health and Vivify have a documented incident management procedure, Incident Management (Vivify & Ontario Health) – Process	The incident management procedure must include steps that Vivify must take when Vivify detects and	Completed

		Improvement Opportunities in place however, a few of gaps have been identified in the procedural document. • The procedure does not include processes for when Vivify detects a privacy and/or security breach and steps that Vivify must take under this scenario (i.e. notification requirements) but instead only includes processes when Ontario Health contacts Vivify for assistance with a privacy and/or security breach. • The process is silent on "containment" requirements for Vivify. In the event that there is a security and/or privacy breach, Vivify should be required to assist in containment of a breach where their assistance is required. • In addition, Vivify is required to provide "root cause" analysis and recommendations, however, Vivify may not always be in a position to do so especially when the investigation and root cause analysis is being handled and led by the host site.	identifies a privacy and/or security breach. The incident management procedure must include requirements including roles and responsibilities around "containment" efforts with respect to privacy and/or security breach. For clarity, the incident management procedure should specify "when" Vivify is required to produce the "root cause" analysis and recommendations. For example, when a privacy and/or security breach is caused by Vivify, Vivify will provide a root cause analysis and their recommendations to Ontario Health.	
7	Medium	Patient end users must be informed of who to contact	Ontario Health and Vivify should provide patients	Completed

		in the event that they suspect a privacy and/or security breach of their PHI. Without easy to access instructions on who to contact there is a risk of delayed response and containment of a privacy and/or security breach.	with easy to access instructions on who to contact in the event that they suspect a privacy and/or security breach. Ideally, this information should be available within the +GO iOS and Android app, as well as the now decommissioned +GO Web App.	
8	Medium	Without clear instructions to patients on how to make an individual access request or make corrections to their PHI, the individual patient's may find it difficult to exercise their right of access and corrections.	Ontario Health and Vivify should consider adding instructions for patients on the +GO iOS and Android app as well as the now decommissioned +GO Web App on how one would go about and make an individual access request and/or request for corrections. Patients should be directed to their respective Health Information Custodian.	Completed

Update: New SMS enhanced functionality will be enabled that was outside the scope of the original PIA assessment and as such an internal Statement of Risk was conducted on *November 19, 2019.*

While the Vivify Remote Patient Management solution is hosted in Ontario and data associated with this component of the solution (provider station and patient mobile device) remains in Ontario, it was identified that the Vivify Go (Mobile Apps) solution stores and transmits some personal health information outside of Canada i.e.: patient mobile number, and any configurable messages to the patient would be transmitted and stored in the United States of America through an application programming interface (API) to Vivify's for Short Message Service (SMS) provider.

Key Findings/Risks & Recommendations

In this Statement of Risk: 9 risks were identified, 3 of which were rated as High, 5 were rated as Medium and 1 rated as Low. Description of risk rating categories follow Ontario

Health's PIA policy which recommends that all high/medium risks be mitigated to an acceptable level prior to a project/initiative 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.

#	Risk Level	Finding/Risk	Recommendation (s)	Status
1	High	Master Services Agreement (MSA) does not authorize transmission and storage of PHI outside of Canada.	Amend the agreement between Ontario Health and Vivify to authorize transmission and storage of PHI outside of Canada for the following data elements: 1. patient cell phone number 2. configurable patient text messages	Completed
2	High	OTNhub Terms of Service (Section G) does not provide language for transmission and storage of PHI outside of Canada.	Amending the OTNhub Terms of Service (Section G: Remote Patient Monitoring) to clearly note language that for Vivify Pathways +Go service offering there will be transmission and storage of PHI (cell phone number and configurable text messages) outside of Canada.	Completed
3	High	Current Patient EULA (end user license agreement) does not include SMS enhanced functionality language.	Amend patient EULA (end user license agreement) to include that SMS messages are transmitted and stored outside of Canada and what this would mean for the patient. Note that the patient retains the option to	Completed

			use either email and/or SMS. Update Recommended Privacy Best Practices for Patients with augmented language around SMS enhanced functionality. Password protect or activate biometrics (like Touch ID) for all devices on which patient has downloaded the app. This will prevent unauthorized users from accessing the app.	
4	Medium	Security technical safeguards of SMS are not known nor addressed	Mitigate all identified technical security risks and recommendations prior to launch of SMS. All security risks have been downgraded from high to medium due to mitigation actions implemented and accept risk.	Accept
5	Medium	Privacy & Remote Care Management, 2019/2020 privacy training for the patient's care team members does not reflect the use of SMS messages nor that certain data elements related to SMS are transmitted and stored outside of Canada. Without updating the training, the patient's care team may not be able to assist patients when they have questions around the use of SMS or need assistance.	Update patient onboarding training materials with same messaging as in EULA.	Completed

6	Medium	Security safeguards, admin/physical and technical document may not be current and up to date.	Update Services and Safeguards to include additional SMS enhancement functionality.	Completed
7.	Medium	Onboarding Script for Clinicians does not address SMS enhanced functionality.	Explain risks with SMS and US data residency and what that means for patient in onboarding script for clinicians.	Completed
8	Medium	Augment Privacy and Security of Mobile device artifact	Direct patients to review host sites Mobile Device Policy. Add to Clinicians and Patients Privacy Best Practice document and Securing you Mobile device tip sheet.	Completed
9	Low	Conflicting messaging leading to confusion for patients, i.e.: Vivify app privacy policy, EULA for patient, Twilio Privacy Statement; Terms of Use, Ontario Health privacy policy.	Describe for the patient in clear concise language how all these different statements and policies are applied in their use of the Vivify Solution. Augment language in Privacy Best Practices for Patients as well as add to Privacy Centre (Consumer Privacy Notice) at otn.ca with what data elements are collected.	Completed

Please contact the Ontario Health Privacy Office should you have any questions.

Email: OH-OTN_privacy@ontariohealth.ca / Phone: 1-855-654-0888
Mail: Ontario Health (Ontario Telemedicine Network)
438 University Avenue, Suite 200
Toronto, ON M5G 2K8