Ontario Health
OTN

Privacy Impact Assessment and Updated Statement of Risk Summary

Privacy Impact Assessment – (Therapy-Assisted Internet-Based Cognitive Behavioural Therapy (Morneau) (TAiCBT)

Date Originally Written: December, 2019
Date Reviewed and Updated: September 2, 2020

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

OTN 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 OTN's products or services. OTN 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 OTN. 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

[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.

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 Privacy Impact Assessment (PIA) on *TAiCBT* dated September 23, 2019**.** The PIA assesses the process by which OTN will collect the data, how OTN plans to use the data, and ensure public trust that OTN handles PHI in a responsible manner. However, for the project that is the subject of this PIA, the intention is to ensure that no PHI is provided by MindBeacon to OTN.

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

Background

OTN will be launching a pilot project in collaboration with the Ministry of Health and Long-Term Care and the Ministry of Training, Colleges and Universities to offer Therapist-Assisted Internet-Based Cognitive Behavioural Therapy ("*TAiCBT*") to four Universities/Colleges in Ontario across five campuses. *TAiCBT* is intended to provide diversified support to students for mild to moderate depression and anxiety.

The BEACON online platform is an application licensed to and operated by MindBeacon Health Inc. ("MindBeacon"). MindBeacon is a Canadian organization with offices in Toronto, Ontario supported by eTherapists, who are licensed masters-level social workers. The BEACON platform provides services in all provinces and territories in both English and French and is built on Microsoft's Azure cloud technology infrastructure.

Students have access to the platform for 52 weeks. Once they are discharged from their treatment course, they will still have access to the platform as passive users. As relapse prevention and for outcome measures, at 3 and 6 months, the platform will send a no-reply e-mail to the student inviting them to log onto the platform.

NOTE: All correspondence between the eTherapist and the student occurs via the BEACON platform.

Ontario Health
OTN

Key Findings/Risks & Recommendations

The privacy analysis of the initiative identified 10 risks. 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. The PIA identified some privacy controls that should be enhanced to support the program. OTN has already closed all of the recommendations.

Risk rating 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	The specific data that the Wellness Centre councillors will see in BEACON regarding referred students, as well as the reports that BEACON will make available to the Most Responsible Person have not yet been determined.	Secure sharing of this sensitive personal health information must be clarified and fully tested prior to launch. All communication will be going through Ontario Shores (hub) through the secure Beacon Platform.	Completed
2	High	Data to be shared with ICES for TAiCBT evaluation purposes, the associated data flow process and frequency, as well as what data linkages will be made by ICES needs to be determined.	Review the privacy policy in light of the project and make necessary adjustments. Data will flow from the MindBeacon Platform to Ontario Shores. Ontario Shores will submit data to DATIS directly.	Completed

#	RATING	FINDING/RISK	RECOMMENDATION/MITIGATION	STATUS
			Data Sharing Agreement between MindBeacon and Ontario Shores was executed on November 26th, 2019.	
3	High	A secure communications methodology between MindBeacon and the University/College Wellness Centres has not been determined or assessed.	All communication between eTherapist, Student, Wellness Centre and MindBeacon will be completed through the MindBeacon secure platform.	Completed
4	High	Documents to support privacy best practice and set out data protection responsibilities need to be put into place. In particular: a) the data sharing agreement between the OSP Hub and MindBeacon; b) the data sharing agreement between ICES and MindBeacon; and c) the initial iCBT student consent form.	Ensure these documents are in place, reviewed by legal counsel, and finalized prior to launch of BEACON with the selected Universities/Colleges. MindBeacon is not sharing any identifiable information with OTN. No data sharing between MindBeacon and University/Colleges. Data Sharing Agreement between MindBeacon and Ontario Shores was executed on November 26th, 2019	Completed
5	Medium	There is no written de-identification/anonymization procedure for statistical analysis/reporting.	A written de-identification/anonymization procedure should be documented and presented to OTN for review.	Completed

#	RATING	FINDING/RISK	RECOMMENDATION/MITIGATION	STATUS
			De-Identification Policy 25.0 has been created by MindBeacon	
6	Medium	MindBeacon's privacy breach management and notification policy does not reference notification to OTN in the context of a privacy breach.	MindBeacon's privacy breach management and notification policy should be amended to address notification to the client/stakeholder, even if OTN is not involved in the breach investigation or corrective actions. Addendum amendment to the SOW executed on November 19th, 2019.	Completed
7	Medium	Two factor authentication should be in place for eTherapists' access to BEACON (particularly contractors who are not working in MindBeacon's offices and using their own computers).	A second security layer to reconfirm the eTherapists' identities should be in place given their access to sensitive data across multiple students. Two factor authentication in place on November 28th, 2019.	Completed
8	Medium	The BEACON platform does not have a session inactivity lockout for eTherapists working remotely.	Session time-outs prevent personal information from being visible on a screen that is left unattended. It is advisable to have a session time-out built into BEACON rather than relying on the computer accessing the platform to lock. Although MindBeacon's computers are set to lock out after 15 minutes of inactivity,	Completed

#	RATING	FINDING/RISK	RECOMMENDATION/MITIGATION	STATUS
			eTherapists who are contractors are asked to set up a time-out on their computers. The MindBeacon platform will force a lock out that cannot be altered.	
9	Low	The PHIPA focused privacy and data security training that has been developed for eTherapists is highly detailed and covers aspects of the law that are not relevant for MindBeacon staff.	It is recommended that MindBeacon staff who will work with students in Ontario receive content that is more suited to their roles. Addendum to the Onboarding and Getting Started Manual for Ontario eTherapists and Psychologists dated May 2019.	Completed
10	Low	E-mails sent to a student automatically by BEACON could result in an inadvertent disclosure of personal health information (the fact that the student uses BEACON) if accessed by anyone other than the student.	The consent for Beacon Platform Account should state that the student's e-mail address must only be accessible by the student, and the e-mail account used for BEACON e-mails should be properly secured. eTherapists do not communicate with students via e-mail – all such interactions are through the platform. However, welcome messages and 3/6-month post-discharge follow up e-mails are sent automatically by the system. Being a BEACON user could in and of itself be	Completed

#	RATING	FINDING/RISK	RECOMMENDATION/MITIGATION	STATUS
			sensitive due to the stigma associated with mental health issues. A just-in-time notice will appear when the student is providing their e-mail address that provides such a warning.	

A **Statement of Risk** was completed on **May 14, 2020 for iCBT Phase 2**. Funded by the Ministry of Health (MOH), this project focused on the procurement and implementation of Therapy Assisted Internet-based Cognitive Behavioural Therapy (TAiCBT) services to healthcare workers and other Ontarians struggling with mental health concerns related to the COVID-19 pandemic. Ontario Health (OTN Business Unit) (OH) will collaborate with other Ontario Health Business Units and external partners to support the creation of a cohesive model and centralized location for Ontarians to access available MOH supported mental health services including iCBT during the pandemic. Both iCBT service providers that were part of phase 1 (MindBeacon and Morneau Shepell) will be part of the phase 2 implementation and expansion.

The following table provides a very high-level summary of the risks/risk ratings, including legal authority, that were identified and assessed as part of our review of the project related documentation and processes. The initial implementation review included a Privacy Impact Assessment (PIA) and a Threat and Risk Assessment (TRA) conducted by an OH Vendor of record on December 30, 2019**. There are no significant design or configuration changes to the solution or integration with other systems in expansion.**

In the Statement of Risk, we have identified **5 privacy risks,** 3 High, 1 Medium and 1 Low. Description of risk rating categories follow OH'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.

#	RATING	FINDING/RISK	RECOMMENDATION/MITIGATION	STATUS
1	High	Existing Statement of Work (SOW) does not include Phase 2 self-referral and expansion and therefore lacks accountability for the vendor on deliverables, costs and timelines.	Amendment to SOW for expanded roll-out beyond colleges and universities. Signed on March 31, 2020.	Completed
2	High	There is risk of non-compliance with PHIPA that Ontarians may not be aware that information is being collected, who will use it and for what purpose (s).	Augment language in consent to include the following: 1. Information collected to be limited to what is truly necessary for the purpose of the iCBT program. 2. "I understand that I may amend, restrict or withdraw my consent or delete my account at any time. Should I choose to do so, I understand that the change to my consent may affect or limit the services that I can access through the MindBeacon platform."	Completed
3	High	Documents to support privacy best practice and set out data protection responsibilities need to be put into place prior to data sharing.	Data Sharing Agreements to be completed and signed off by all parties prior to sending any **de-identified, aggregated data.** a) DSA required for The Royal Mental Health – Care and Research b) DSA required with DATIS (for self-referral process)	In Progress In Progress

Ontario Health
OTN

#	RATING	FINDING/RISK	RECOMMENDATION/MITIGATION	STATUS
			c) Notify user in consent of purpose of sharing their de-identified data No identifiable data will be shared between MindBeacon and OH.	Completed
4	Medium	Ontarians may lose trust in dealing with OH and Service Provider if needs cannot be met in a timely manner if determined client does not require iCBT or needs to be stepped up. Ultimately leading to a lack of engagement that may affect reputation of organization.	Develop a "step up" "step out" documented process and resource list to aid clinicians in determining what are appropriate alternatives to refer clients to.	Completed
5	Low	Ontarians may not be familiar with best practices in a virtual environment and how to secure their mobile devices to prevent malicious activity and risks.	Create a best practice document for clients in a virtual environment with tips on how to secure their mobile device.	Completed

Please contact the OTN Privacy Office should you have any questions:
Email: privacy@otn.ca