Privacy Impact Assessment Summary

Project Name: **Substance Use Disorder (SUD)**
Date Originally Written: October 6, 2021
Date Reviewed and Updated:

A Privacy Impact Assessment (PIA) is a risk management tool that allows the 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. 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 *Substance Use Disorder project*, key findings & recommendations, target date for completion, and contact information for the OH Privacy Office.

Background

As a result of the COVID-19 pandemic, the issues around the ability to access treatment for substance use disorders (SUD) has only been compounded, leading to modified or reduced ability to receive in-person treatment. As a result of the current difficulties involved in receiving in-person treatment, the Ontario government has committed to investing in expanding mental health and addiction services to support individuals negatively impacted by the pandemic due to issues such as social isolation and lack of accessibility to services.

[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.

It is in this context that OH has asked an external PIA Consultant to conduct a Privacy Impact Assessment of Breaking Free's internet-based, self-directed cognitive behavioural therapy platform, which has been chosen as the solution that is being deployed province-wide to address access to SUD-based resources and self-directed therapy. Breaking Free Online Limited (whose trade name is "Breaking Free Group", referenced as "Breaking Free") has developed a web-based platform and mobile application that provides individuals with access to a toolkit of psychoeducation, recovery resources, and evidence-based behaviour change techniques. It has been designed to support individuals to achieve and maintain recovery from, and dependence on over 70 substances (e.g., opioids, stimulants, prescribed medications, and alcohol) whilst also targeting concurrent mental difficulties such as anxiety and depression.

Following an examination of solution and business architecture documents, along with privacy and security legal provisions, the Privacy Impact Assessment informed the following findings:

- The purpose and use of personal health information to be held within the Breaking Free solution pertains to the provision of self-directed cognitive behavioural therapy for substance use disorders for individuals across Ontario.
- Breaking Free will obtain consent from each individual prior to registering an account with Breaking Free. A risk exists involving the sufficiency of the consent notice in terms of providing individuals with information regarding the purposes for Breaking Free's collection, use and disclosure of personal health information.
- The Master Agreement between OH and Breaking Free contains appropriate legal provisions concerning data residency, breach notification, and the maintenance of appropriate security measures to protect personal data held with Breaking Free. The agreement does not specify the responsibilities of Breaking Free or OH.
- The Breaking Free application is being hosted by Digital Ocean in an Equinix co-location data centre located in Toronto. Patient data is held within Google Service Cloud's data centre in Montreal, with backups being stored in Mongo DB's clustered Canadian data centres.
- Breaking Free, for the purposes of the *Personal Health Information Protection Act (PHIPA) and regulation,* is considered a health information custodian.
- Based on the information provided, no PHIPA violations have been noted. However, there remains a number of "unknowns" regarding the contractual relationships between (i) Breaking Free and its call centre, AnswerPlus; (ii) Breaking Free and its cloud service providers, and (iii) the nature of the involvement of a subcontractor in the provision of its services. These "unknowns" could lend themselves to PHIPA violations, and further information is required to fully assess the initiative's compliance with PHIPA.
- The flow of personal health information outside of the Breaking Free solution amongst OH stakeholders as it relates to evaluation of the program requires further definition.

Key Findings/Risks & Recommendations

The privacy analysis of the initiative identified thirteen (13) risks. OH'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:

#	RATING	FINDING/RISK	RECOMMENDATION/MITIGATION	STATUS
1	Medium	There is a lack of certainty as to the types of aggregated or de-identified information OH will be receiving from Breaking Free, and whether there is any identifying information within those data sets.	OH should have data sharing agreements in place with its stakeholders, including Breaking Free. While no identifiable personal health information will be shared, the data sharing agreements should set out the purposes for the data sharing, covers what happens to the data at each stage (e.g., de-identification/re-identification, analysis, evaluation), set standards and clarify the roles and responsibilities for the parties involved in the sharing of data. OH has indicated that OH and Breaking Free will be revising their legal agreements to include these data sharing provisions.	COMPLETE
2.	Medium	Lack of Protocols for Distribution of Information	OH should consider developing internal processes with its stakeholders involved in this initiative that defines the types of data they will receive, on what frequency, the safeguards to be implemented, and the purposes for which data may be used for. (See #1)	COMPLETE
3.	Medium	Lack of Guidance Provided to Health Service Providers (HSPs) Regarding the Safeguarding of Aggregated Reports	Breaking Free to develop guidance for HSPs for instances where they are designated as a supporter by their patient, and how to safeguard the information in the reports generated by Breaking Free. Breaking Free has indicated that guidance will be added to the Breaking Free Toolkit.	COMPLETE
4.	Medium	Risk of Patient Re-Identification	OH may wish to reconsider which data elements they receive from Breaking Free in order to avoid any risk of patient re-identification. Alternatively, OH may wish to develop internal processes to ensure that where re-identification is possible, that certain identifiers that may be linked together are removed from any analysis done by OH (e.g.,	COMPLETE

#	RATING	FINDING/RISK	RECOMMENDATION/MITIGATION	STATUS
			removing date of birth from a particular analysis).	
5.	Medium	Risk of Patient Information Being Sent to Incorrect 'Supporter' E-mail Address	Breaking Free should consider requiring the individual to verify the supporter's e-mail address in order to avoid sending patient information to unintended recipients, should the individual mistakenly enter the wrong e-mail address.	COMPLETE
6.	Medium	Risk of Unauthorized PHI Disclosure	Email messages containing PHI will be sent to Supporters. This should be done as securely as possible or, where not feasible, with the explicit knowledge and consent of Patients. For example, one alternative could be to provide a secure link/passcode shared with them by the individual in order to access the reports that are being shared. Another alternative, may be to wish to consider implementing a "pop-up" message for patients prior to reports being sent out to supporters. confirming that they wish to send a report containing personal health information to their supporter via e-mail.	COMPLETE
7.	Medium	Insufficient Consent Notice	Breaking Free should consider incorporating some of their privacy policy language into their consent notice or developing a plain language consent notice that states the types of personal health information collected, the purposes for which PHI is collected, used (e.g., research purposes), and disclosed (e.g., to which organizations) and that a patient may withhold their consent. This includes when obtaining consent within the mobile application. Breaking Free will be developing a document to address gaps in Breaking Free's consent and privacy policy.	COMPLETE

#	RATING	FINDING/RISK	RECOMMENDATION/MITIGATION	STATUS
8.	Medium	Insufficient Breach Notification Requirements	Breaking Free should amend their Privacy Breach and Incident Management Protocol to respond to legislative requirements as a Health Information Custodian (HIC) under PHIPA that requires, with respect to notification of affected individuals, in order to ensure compliance with relevant legislation. Incident response plans should incorporate considerations for when a breach affects more than one HSPs patients and who is responsible (i.e., Breaking Free or the HSP) for notifying affected individuals. OH may also wish to consider requesting that Breaking Free share any agreements it has with OH where the services relate to providing the SUD solution in Ontario.	COMPLETE
9.	Medium	Lack of Terms of Service	Breaking Free should consider developing a Terms of Service that patients must consent to upon registration with Breaking Free, that defines the terms upon which the service is being provided to individuals in Ontario, and clarification of Breaking Free's role in the provision of its service. Breaking Free should also develop a Terms of Service for Health Care providers that addresses gaps and notifies them of obligations of parties.	COMPLETE
10.	Low	The collection of geo-location data is not defined in Breaking Free's Privacy Policy.	Breaking Free should include the collection of geo-location through the use of Google Maps API in Breaking Free's Privacy Statement. OH has indicated that they have asked Breaking Free to update their FAQ page to include information about the Google Maps API and how geo-location is being used.	COMPLETE
11.	Low	No mechanism for collecting parental consents where youths	Breaking Free should develop a mechanism for obtaining parental	COMPLETE

#	RATING	FINDING/RISK	RECOMMENDATION/MITIGATION	STATUS
		register themselves for Breaking independently through the "direct-to-consumer" model.	consents or a notice that site is meant for patients aged 16 and over.	
12.	Low	Insufficient Access, Correction and Complaint Procedure	Breaking Free should consider developing an Access and Correction Policy and Procedure that sets out Breaking Free's access procedures in compliance with PHIPA. Breaking Free's Access procedure should also contemplate how they handle requests that come in from HSPs or other referring agencies. The access procedure should be included in Breaking Free's Privacy Policy. Breaking Free should also clarify on its website how privacy complaints will be handled and to whom complaints should be directed to.	COMPLETE
13.	Low	Non-Compliance with Archives and Recordkeeping Act	OH should consider amending its retention policies to reflect the collection of Breaking Free data, both the aggregated data sets received, as well as any derivative works or research resulting from the data sets received. Breaking Free will also be addressing the retention of aggregated reports generated for OH.	IN PROGRESS

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 / 1-855-654-0888 / TTY: 1-855-368-6889 / Fax: 416-446-4139