Mental Health Commission of Canada
Commission de la santé mentale du Canada

Assessment Framework for Mental Health Apps

Ce document est disponible en français

Citation information
Suggested citation:

Mental Health Commission of Canada. (2023). *Assessment framework for mental health apps*.
https://mentalhealthcommission.ca

The views represented herein solely represent the views of the Mental Health Commission of Canada.

ISBN: 978-1-77318-305-3

Legal deposit National Library of Canada

Health Canada Santé Canada

The views represented herein solely represent the views of the Mental Health Commission of Canada. Production of this material is made possible through a financial contribution from Health Canada.

Contents

Acknowledgments

Stakeholders

The Mental Health Commission of Canada engaged with nearly 200 stakeholders in various roles and perspectives, which included policy and research, persons with lived and living experience, providers, health executives, app developers, and app designers. This public review document would have not been possible without their valuable contributions.

Core Development Team

Mental Health Commission of Canada

- Nicholas Watters — Director, Access to Quality Mental Health Services
- Maureen Abbott — Manager, Access to Quality Mental Health Services
- Sapna Wadhawan — Program Manager, Access to Quality Mental Health Services
- Kelsey Kavic — Program Coordinator, Access to Quality Mental Health Services
- Al Raimundo — Adviser

ORCHA

- Tim Andrews — Chief Operating Officer
- Nii Lante Wallace-Davies — Vice-President of Customer Success
- Saira Arif — Customer Success Manager
- Rachel Fuller — Project Manager
- Leyla Sollitt — Lead Digital Health Assessor

Glossary of Terms, Abbreviations, and Acronyms

ADA. *Americans with Disabilities Act* Standards for Accessible Design.

adult. People 19 and older (according to the Office of the Privacy Commissioner of Canada).

AI. Artificial intelligence refers to the simulation of human intelligence processes by machines. In this document, AI will be identified if the expert systems, natural language processing, speech recognition, or machine learning use the inputted mental health data; for example, a chatbot that was programmed to discuss the user's mental health with them.

algorithm. Mathematical calculations that produce outputs, providing further insight into the mental health data it manipulates; for instance, calculating the average mood recorded by the user in a given week.

Android Application Quality Guidelines. A checklist that defines core criteria and tests to help developers assess the quality of their app while highlighting the minimum quality that all apps should meet.

AODA. *Accessibility for Ontarians with Disabilities Act*.

API. Application programming interface.

APMG. A firm that accredits organizations to deliver high-quality cybersecurity training courses.

Apple HIG. Apple human interface guidelines.

apps/applications. Refers to the relevant digital health product.

assessment framework. A set structure of standards and criteria.

assessor. An individual trained to carry out the MHCC's assessment against the assessment framework.

behaviour change. Refers to behaviour change techniques apps may adopt to deliver or achieve a specific outcome. Cognitive behaviour therapy (CBT) and dialectical behaviour therapy (DBT) are examples of such techniques.

BIPOC. Black, Indigenous, and people of colour.

charity. A charitable organization, public foundation, or private foundation registered with the Canada Revenue Agency.

CHECK. The term for National Cyber Security Centre-approved companies that can conduct authorized penetration tests of state-sector applications.

children. Persons below age 13 (according to the Office of the Privacy Commissioner of Canada).

CIS Top 20 Compliance. The Centre for Internet Security (CIS) Top 20 Critical Security Controls is a prioritized set of best practices created to protect against today's most dangerous cyber threats.

co-design. In this document, refers to having a person (or people) with lived and living experience as a designer of an app. Kleinsmann and Valkenburg describe co-design as "the process in which actors from different disciplines share their knowledge about both the design process and the design content. . .to create shared understanding on both aspects [and] achieve the larger common objective: the new product to be designed (p. 30)."[1]

cookies. Small text files containing information generated by a server when a web connection is established and placed on a user's or visitor's personal computer or smart device.

community. A social unit with commonality such as norms, religion, values, customs, or identity.

company. A software company is a company whose primary products are various forms of software, software technology, distribution and software product development.

CREST. CREST accreditation demonstrates that a company conducts and documents penetration testing (i.e., an authorized simulated cyberattack on a computer system, performed to evaluate its security) in accordance with the highest legal, ethical, and technical standards.

criteria. Carefully chosen principles that apps are assessed against. In this document, each criteria is phrased as a question. The list of criteria formulates every standard and makes up the overall assessment framework.

CSS. Clinical specialty systems that specialize in a particular health problem, which are usually placed in different areas of a hospital. For example, the maternity ward would have a maternity clinical specialty system to record important information.

CyberSecure Canada. A national program that enables small and medium-sized organizations to achieve certification. To do so, they must implement requirements to protect their business, users, and partners from cyberattacks.

data management standards. Standards that set out guidelines by which data are described and recorded. Adhering to data management standards ensures that a company is following best practices in handling their data.

---

[1] Kleinsmann, M., & Valkenburg, R. (2008). Barriers and enablers for creating shared understanding in co-design projects, *Design Studies, 29*(4), 369-386. https://doi.org/10.1016/j.destud.2008.03.003

data subjects. The identified or identifiable individual that personal data relates to.

developer. The person or people who created and developed a mobile or web application.

digital health product. Mobile or web-based applications.

EHRs. Electronic health-care records that are accessible across a range of services, i.e., the same record is accessible from the family doctor and from the hospital.

EMRs. Electronic medical records that are only accessible by one service, i.e., a record maintained and accessed only at one family doctor's office.

encryption. A method of converting information into secret code that hides its true meaning. Data that is encrypted is viewed as secure.

ESF. The evidence standards framework developed by the National Institute for Health and Care Excellence (NICE) for digital health technologies, made up of effectiveness and economic impact standards.

ethnic. A population group with a common national or cultural tradition.

federal government organization. Institutions created to regulate industries or practices that require specialized expertise or general oversight.

FNIGC. First Nations Information Governance Centre.

GDPR. The *General Data Protection Regulation* is the standard developed in the United Kingdom (U.K.) and the European Union (EU). All apps must be fully compliant with this standard.

general health/wellness. A broad term used to highlight non-specific mental health problems, e.g., non-specific stress.

Indigenous peoples. The collective name adopted by the government of Canada "for the original peoples of North America and their descendants" (para. 1).[2]

in vitro diagnostic devices (IVDs). Devices that test biological samples such as tissues, blood, or urine.

ISO 25062. A framework that provides a standard method for reporting usability test findings collected through quantitative measurements. It is particularly appropriate for summative/comparative testing.

ISO 27001. A widely known framework that provides requirements for an information security management system.

[2] Crown-Indigenous Relations, & Northern Affairs Canada. (2021). *Indigenous peoples and communities*. https://www.rcaanc-cirnac.gc.ca/eng/1100100013785/1529102490303

ISO 9241. A framework for understanding the concept of usability and applying it to situations in which people use interactive systems.

jurisdictional principles. Rules set by a state that explain or control how something happens or works and how these elements affect persons, property, and circumstances in its geographical territory.

lived experience/living experience. Personal knowledge about the world gained through "direct, first-hand involvement in everyday events rather than through representations constructed by other people."[3] The term has also been defined as "the experiences of people on whom a social issue or combination of issues has had a direct impact" (p. 6).[4]

machine learning. This document considers machine learning a technique of AI. After the assessor has determined that an app uses AI, the framework asks which AI technique is involved. Responses include machine learning, natural language processing, etc.

MAUQ. Mobile health app usability questionnaire.

medical device. Any instrument or component used to treat, diagnose, or prevent a disease or abnormal physical condition.

mental health problem. A consistently used phrase throughout this framework to denote the full range of mental health conditions that affect people.

medical purpose. Please refer to the definition of 'device' in the Food and Drugs Act, where medical purpose includes those elements listed in (a) through (e).

MHCC. The Mental Health Commission of Canada.

NHS. The National Health Service is England's publicly funded health-care system.

NICE. The National Institute for Health and Care Excellence is an executive non-departmental public body in the Department of Health and Social Care (U.K.).

ORCHA. The Organisation for the Review of Care and Health Apps.

OCSA. The ORCHA clinical safety assessment is a set of criteria developed to objectively outline safety considerations for health app developers to adhere to.

OCAP. First Nations principles of ownership, control, access, and possession that reflect their commitment to use and share information in a way that benefits the community while minimizing harm.

---

[3] Chandler, D., & Munday, R. (2020). Lived experience. In *Oxford: A dictionary of media and communication* (3rd ed.). Oxford University Press. https://doi.org/10.1093/acref/9780199568758.001.0001

[4] Sandu, B. (2017). *The value of lived experience in social change: The need for leadership and organisational development in the social sector*. http://thelivedexperience.org/report/

organization. A company, charity, insurer, or provider involved in the mental health and physical health care or therapeutic space.

OWASP level. The Open Web Application Security Project Application Security Verification Standard (ASVS) is a framework that focuses on defining security controls. Each application is assigned an OWASP level based on particular qualities. Evidence is then reviewed proportionally against that assigned level.

PEN/vulnerability — penetration/vulnerability testing. A simulated cyberattack against your computer system to check for exploitable vulnerabilities.

person with disability. A group that includes "those who have long-term physical, mental, intellectual or sensory impairments which in interaction with various barriers may hinder their full and effective participation in society on an equal basis with others" (p. 3).[5]

PHI. Protected health information, which is any "identifying information" about an individual, whether oral or recorded, that relates to (1) the individual's mental health problems, including family medical history, (2) the provision of health care or a plan of service for the individual, (3) payments or eligibility for health care or its coverage, or (4) the donation of any body part or bodily substance or the testing or examination of any such part or substance. PHI also includes the individual's health number and the identification of a health-care provider or substitute decision maker for the individual.

PHRs. Personal health records give people access to their own medical histories.

PII. Personally identifiable information can identify an individual, either used alone or with other relevant data.

PIPEDA (or Privacy Act). The *Personal Information Protection and Electronic Documents Act* is a Canadian law relating to data privacy. It governs how private sector organizations collect, use, and disclose personal information in the course of doing business.

provincial or territorial government or representative. Government bodies created to regulate industries or practices that require specialized expertise or general oversight.

RCT. A randomized control trial is considered a high-quality study. They enable apps to be tested against a control whereby participants are randomly placed in an experimental or control group.

SaMD. Software as a Medical Device is a Health Canada term to identify software used for one or more medical purposes.

signal acquisition system. A system that acquires real-world, user-derived, data that can serve as input to the SaMD.

---

[5] United Nations Convention of the Rights of Persons with Disabilities, December 6, 2006, https://www.un.org/disabilities/documents/convention/convention_accessible_pdf.pdf

SOC-2. An auditing procedure to ensure that service providers securely manage data.

therapeutic support. Support with a person's circumstances or mental health problem (as opposed to technical issues).

2SLGBTQ+. Two spirit, lesbian, gay, bisexual, transgender, queer and/or questioning and additional sexual orientations and gender identities.

US DHAF. The U.S. Digital Health Assessment Framework, which ORCHA developed with the American Telemedicine Association.

WC3. World Wide Web Consortium.

WCAG 2.0 AA. Web Content Accessibility Guidelines 2.0 AA.

WCAG 2.1 AA. Web Content Accessibility Guidelines 2.1 AA.

youth. People ages 13 to 18 (according to the Office of the Privacy Commissioner of Canada).

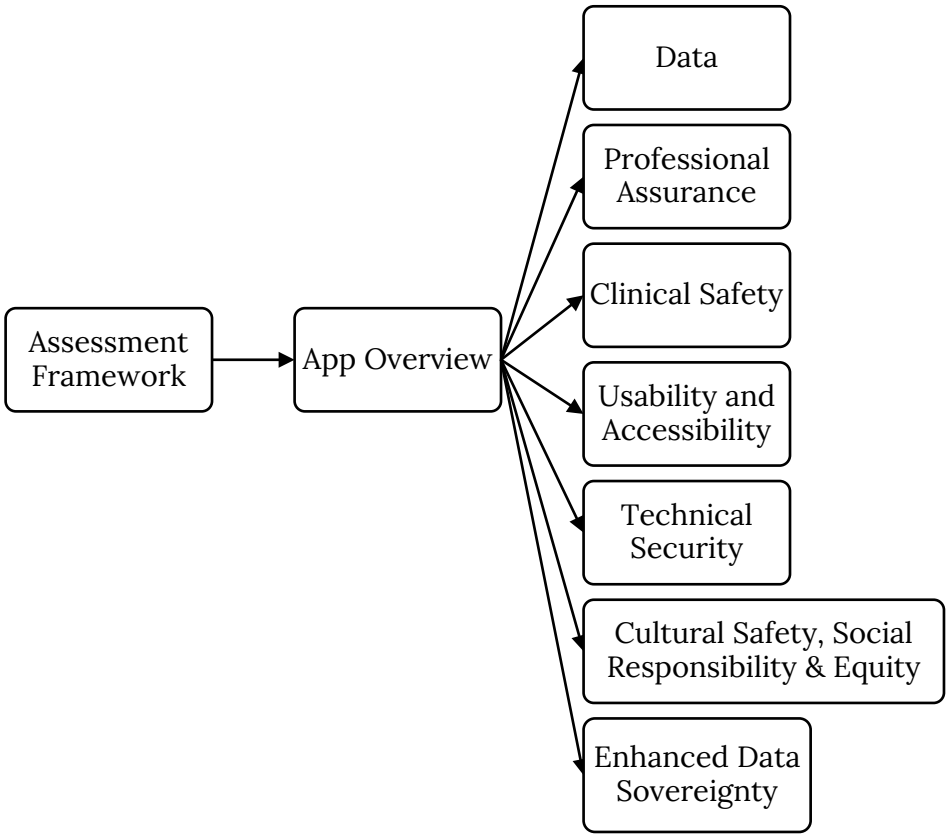
Assessment Framework Structure

Assessment framework. A document that contains a set structure of standards and criteria.

Standards. A specific, focused area or topic made up of a list of relevant criteria.

Criteria. Carefully chosen principles that apps are assessed against. Criteria are currently phrased as questions. A list of criteria formulates every standard and makes up the overall assessment framework.

Figure 1. Assessment Framework Diagram



Example of the structure:

2. Data and privacy standards = standards
2a. Privacy policy = a set of criteria

Figure 2. List of Criteria

	Criteria	Criteria Origin
2a — Q1	Is there a privacy policy available via the web app/website? (only relevant for web apps)	ORCHA
2a — Q2	Is a privacy summary published anywhere by the developer? (only relevant to mobile apps)	ORCHA
2a — Q3	Is the privacy policy made immediately available when the user first opens the app?	ORCHA

1. App Overview

This assessment framework begins with the app overview. The criteria listed below (grouped into distinct areas) aim to understand an application's core purpose and functionality. These include the target audience, the type of data the app collects, and the app's primary functions and features. Because these criteria do not have scoring implications, the application will not be scored based on its functionality. Instead, the criteria will effectively set the scene and inform the standards criteria that need to be posed for that specific application.

1a. Application characteristics

	Criteria	Criteria Origin
1a — Q1	Is the application mental health focused?	MHCC

1b. Data — Data types, data collection, and data sharing

	Criteria	Criteria Origin
1b — Q1	Does the application collect data?	ORCHA
1b — Q2	What type of data is collected by the app?	ORCHA
1b — Q3	Are users required to sign up/register to use the service?	ORCHA
1b — Q4	Is data collected through cookies?	ORCHA
1b — Q5	What type of cookies are used?	ORCHA
1b — Q6	Is the data (cookie and/or none cookie) collected sensitive, personal, and/or non-personal?	ORCHA
1b — Q7	How is none cookie data collected?	ORCHA
1b — Q8	What other apps is the application connected to?	ORCHA
1b — Q9	What device(s) does the application connect to?	ORCHA
1b — Q10	Can the user prevent cookie data from being collected and still use the app?	ORCHA

	Criteria	Criteria Origin
1b — Q11	Does the disabling of cookies impact the use of the application in any way?	ORCHA
1b — Q12	Can/is data shared (excluding cookies)?	ORCHA
1b — Q13	Can data be shared through a direct, manual action by the user (e.g., by sending data via email or manually choosing to post/share something within the application)?	ORCHA
1b — Q14	How is the user able to manually share their data?	ORCHA
1b — Q15	Is data *only* shareable through a direct, manual action by the user (excluding cookies)?	ORCHA
1b — Q16	Can the user control any automatic data sharing, through setting individual sharing preferences in the app (excluding cookies)?	ORCHA
1b — Q17	Where/with whom can the user share data automatically by manually setting sharing preferences in the app?	ORCHA
1b — Q18	Is any data (excluding cookie data) shared automatically as soon as the application is accessed — based only on agreement to relevant terms and conditions (T&Cs) or privacy policy?	ORCHA
1b — Q19	Where/with whom is data automatically shared — based only on user agreement to the developer's privacy policy and/or T&Cs?	ORCHA
1b — Q20	What data is automatically shared with the developer?	ORCHA
1b — Q21	What data is automatically shared with clinicians/health-care professionals?	ORCHA
1b — Q22	What data is automatically shared with other users?	ORCHA
1b — Q23	What data is automatically shared with third parties?	ORCHA
1b — Q24	What data is automatically shared with other devices?	ORCHA
1b — Q25	Is the service/provider a federal government organization listed with Canada's *Privacy Act*?	MHCC
1b — Q26	Is the service/provider a provincial or territorial government or an agent of a provincial or territorial government?	MHCC
1b — Q27	Is the service/provider a charity?	MHCC

	Criteria	Criteria Origin
1b — Q28	Is the organization a not-for-profit group that does not engage in any commercial activities (e.g., sports associations, professional associations, clubs)?	MHCC
1b — Q29	Is the product aimed at or likely to be used by Indigenous people in Canada?	MHCC
1b — Q30	Will the organization collect and process personal information from Indigenous users?	MHCC

1c. Algorithm/AI

	Criteria	Criteria Origin
1c — Q1	Does the application contain algorithms?	ORCHA
1c — Q2	How does the application use the algorithm?	ORCHA
1c — Q3	Does the application appear to use artificial intelligence (AI)?	ORCHA
1c — Q4	What AI technique is used in the app?	ORCHA
1c — Q5	Is the AI monitored/maintained?	ORCHA

1d. Information

	Criteria	Criteria Origin
1d — Q1	Is the application designed to provide information or guidance?	ORCHA
1d — Q2	Does the application provide information that is personalized to an end-user's specific circumstances?	ORCHA
1d — Q3	Does the application provide users with information regarding where they are able to find local or suitable support services?	ORCHA
1d — Q4	Does the application provide information, resources, or activities to the public or clinicians, either about a specific mental health problem or general health and lifestyle?	ORCHA

1e. Clinical decision support — Pre-diagnosis, diagnosis, and treatment support

	Criteria	Criteria Origin
1e — Q1	Is the data the application collects automatically assessed for the purposes of evaluating • risk or • providing diagnostic support?	ORCHA
1e — Q2	Does the application provide an assessment (of the risk) to an individual based on data input or collected by the application of • living with a mental health problem • the impact on their lifestyle and health indicators • no risk assessment provided?	ORCHA
1e — Q3	Does the application provide an assessment (of the risk) to a health-care professional based on data input or collected by the application of • living with a mental health problem • the impact on their lifestyle and health indicators • no risk assessment provided?	ORCHA
1e — Q4	Does the application provide the option for further assessment or analysis by a health-care professional?	ORCHA
1e — Q5	Is the app/does the application include a symptom checker?	ORCHA
1e — Q6	Does the application discuss suicidal ideation? **Guidance:** The CDC (Centers for Disease Control and Prevention) defines suicidal ideation as thinking about, considering, or planning suicide. Machine learning techniques that feature engineering or deep learning for automatic detection (based on online social contents) is one means for detecting suicidal ideation.	MHCC
1e — Q7	Does the application indicate likelihood of a match for the listed mental health problems?	ORCHA

	Criteria	Criteria Origin
1e — Q8	Can users filter results to display by highest risk/likelihood/severity?	ORCHA
1e — Q9	Does the application provide treatment recommendations for the listed mental health problems?	ORCHA
1e — Q10	Does the application only signpost the user to suitable care or recommend seeking further advice (e.g., Go to A&E, book an appointment with your family doctor, call 911)?	ORCHA
1e — Q11	Does the application contain a clinical calculator?	ORCHA
1e — Q12	What type of clinical calculator does the application contain?	ORCHA
1e — Q13	How does the application prevent disease?	ORCHA
1e — Q14	What treatment does the application provide?	ORCHA
1e — Q15	Does the application guide the treatment of a mental health problem?	ORCHA
1e — Q16	How does the application guide the treatment of the mental health problem?	ORCHA
1e — Q17	Who does the application provide the treatment guidance to?	ORCHA
1e — Q18	Is the treatment provided independently of a health-care professional?	ORCHA
1e — Q19	Does the application support health-care professionals' decisions about treatments?	ORCHA
1e — Q20	Does the application follow the path of a procedure/treatment without making any decisions?	ORCHA
1e — Q21	Does a health-care professional make the final decision regarding treatment based on advice and/or options displayed?	ORCHA
1e — Q22	Does the application automate the treatment pathway for an individual user?	ORCHA
1e — Q23	Is the application intended to (or does the developer claim it can be used to) compensate a mental health problem?	ORCHA
1e — Q24	Does the application predict the fertile window?	ORCHA

	Criteria	Criteria Origin
1e — Q25	Does the application claim to be used to prevent pregnancy or to conceive?	ORCHA
1e — Q26	Does the application use body basal temperature (BBT), recorded through an externally connected thermometer?	ORCHA
1e — Q27	Does the application use rhythm, BBT and cervical mucus methods to prevent pregnancy or to conceive?	ORCHA
1e — Q28	Does the developer claim that the application can be used as a natural method of birth control?	ORCHA
1e — Q29	Is the application intended to be used for the control of conception?	ORCHA
1e — Q30	Is the application used in combination with drugs or medication (e.g., medication reminders)?	ORCHA
1e — Q31	Is the application a companion of the device, as opposed to having been designed to connect with a third-party manufacturer's device?	ORCHA

1f. Monitoring

	Criteria	Criteria Origin
1f — Q1	Does the application allow the monitoring of key health information?	ORCHA
1f — Q2	Does the application involve the recording of relevant data over time for the user to access and review (with no "intelligent" manipulation of that data by the app)?	ORCHA
1f — Q3	Does the application involve the automated assessment or interpretation of relevant data to deliver alerts, insights, reminders, or adjustments regarding the management of a specific mental health problem?	ORCHA
1f — Q4	Is the application simple self-management, enhanced self-management, or advanced self-management?	ORCHA
1f — Q5	Is the output of the application's monitoring intended to affect the treatment of an individual?	ORCHA

	Criteria	Criteria Origin
1f — Q6	Does the application allow others (i.e., not the user) to monitor or view the health data captured?	ORCHA
1f — Q7	Does the application automatically measure and/or record data about a user's specified mental health problem and transmit the data to a professional, carer, or third-party organization without any input from the user?	ORCHA
1f — Q8	Does the application generate any alarms or alerts from the data recorded by the application or a connected device?	ORCHA
1f — Q9	Are the alarms generated by user-defined filtering rules?	ORCHA
1f — Q10	What type of intervention or treatment does the application provide?	ORCHA

1.g Online consultations

	Criteria	Criteria Origin
1g — Q1	Can the application be used by users to have online consultations, conversations, or related health-care services with a health-care professional?	ORCHA
1g — Q2	Is this through video consultation?	ORCHA
1g — Q3	Does the application allow health-care professionals to provide clinical advice, as opposed to the application providing advice itself?	ORCHA
1g — Q4	If the application allows health-care professionals to provide clinical advice through the app, rather than the application providing the advice itself, how does it do this?	ORCHA
1g — Q5	Are licensed health-care professionals involved in the delivery of the app?	MHCC

1h. Administrative services

	Criteria	Criteria Origin
1h — Q1	Is this an administrative application which does not directly impact user care?	ORCHA
1h — Q2	What administrative functions does the application provide?	ORCHA
1h — Q3	Is the application used to facilitate communication between health-care professionals other than for consultation or the delivery of advice?	ORCHA
1h — Q4	Does the application allow users to book appointments with a health-care professional?	ORCHA

1i. Pharmacy

	Criteria	Criteria Origin
1i — Q1	Does the application allow users to order and request prescriptions?	ORCHA
1i — Q2	Does the application constitute a pharmacy service?	ORCHA

1j. Reminders/Notifications

	Criteria	Criteria Origin
1j — Q1	Does the application send push notifications?	ORCHA
1j — Q2	Does the application send email notifications?	ORCHA

1k. External device

	Criteria	Criteria Origin
1k — Q1	Is the application's main functionality dependent on the user having one of the devices to connect with the app?	ORCHA

	Criteria	Criteria Origin
1k — Q2	Do any of the features or functions of the application appear to allow it to be used to control a device?	ORCHA

1l. Forums and contacts

	Criteria	Criteria Origin
1l — Q1	Are there opportunities to link with other users (buddying, forums, or group education)?	ORCHA
1l — Q2	Does the application provide an internally hosted forum or online community for their users?	ORCHA
1l — Q3	Does the application link to a third-party service to host a forum or online community for their users?	ORCHA
1l — Q4	Does the application allow two-way communication between citizens or health-care professionals?	ORCHA

1m. Goal setting

	Criteria	Criteria Origin
1m — Q1	Does the application provide gamification or goal-setting features for the user?	ORCHA
1m — Q2	Does the application set goals for the user?	ORCHA
1m — Q3	Does the application allow the user to set goals for themselves?	ORCHA

1n. Customization

	Criteria	Criteria Origin
1n — Q1	Can the application presentation be customized by the user?	ORCHA
1n — Q2	Does the application respond to preferences in the device?	ORCHA

1o. Business model

	Criteria	Criteria Origin
1o — Q1	Is the application totally free?	ORCHA
1o — Q2	How is the application funded?	ORCHA
1o — Q3	Does the application contain advertisements?	ORCHA

1p. Benefits

	Criteria	Criteria Origin
1p — Q1	Are the objectives clearly stated by the app/developer?	MHCC
1p — Q2	What are the claimed or implied benefits of the app? • cost savings to the health-care system • increased access to care • improved diagnostic or risk assessment • improved quality of treatment • improved recovery • reduced readmission or re-referral • improved management of a mental health problem • preventive behaviour change • improved mental well-being • improved physical well-being • improved system/process efficiency	ORCHA
1p — Q3	Has the developer clearly stated the application's target audience?	MHCC
1p — Q4	If the developer has clearly stated the application's target audience, who is the target audience?	MHCC

2. Data and Privacy Standards

Initially, the standards identify the relevant privacy policy for the app, which is available to users through the application itself and/or the Apple App Store or Google Play Store. The more transparent the privacy policy, the better. In general, it must clearly state that user data will not be used or shared with other parties, except as described in the privacy policy or without the express consent of the user. Ideally, it will identify

- what data is collected from the user and how
- if the user is informed of the developer's intentions with processing and sharing their data
- if the user's consent is obtained.

The privacy policy should accurately reflect the data usage of the application. Additionally, it should inform users of the developer's intent to use their data for marketing purposes. If user data is shared for any other purposes than basic use of the app or legal obligations, then the review considers whether the user is able to opt out of these activities.

The data and privacy criteria are listed throughout this section.

2a. Privacy policy

	Criteria	Criteria Origin
2a — Q1	Is there a privacy policy available via the web app/website? (only relevant for web apps)	ORCHA
2a — Q2	Is there a privacy summary published anywhere by the developer? (only relevant to mobile apps)	ORCHA
2a — Q3	Is the privacy policy made immediately available when the user first opens the app?	ORCHA
2a — Q4	Is the privacy policy made available when the user is signing up to the service?	ORCHA
2a — Q5	Is the privacy policy published within the app?	ORCHA
2a — Q6	Is the privacy policy available externally via the app, or via a linked website?	ORCHA
2a — Q7	Is the privacy policy available via the relevant application store?	ORCHA

	Criteria	Criteria Origin
2a — Q8	Is the privacy policy placed in another prominent location that is easily accessible?	US DHAF
2a — Q9	Where can the privacy policy be accessed? **Guidance:** Look for a link to the privacy policy. If one does not exist, does the developer describe how users can obtain the policy, whether through the app or upon request?	MHCC
2a — Q10	Does the privacy policy state what data the developer collects?	ORCHA
2a — Q11	Is the privacy policy accurate, with regards to the data the developer intends to collect?	ORCHA
2a — Q12	Does the application explicitly state that data collected by the application is stored locally unless the user manually exports the data?	ORCHA
2a — Q13	How does the developer obtain consent for the processing of user data?	ORCHA
2a — Q14	Does the privacy policy provide the name and contact details of their privacy officer or similar individual representative for the company?	ORCHA
2a — Q15	Provide the details of the representative who was identified in 2a-Q14.	ORCHA

2b. Data use

Once the kinds of data collected by the app is established, the standards look at how that data is used and shared and whether this is communicated to the user. The privacy policy should state all intended uses and legal bases for processing user data, such as legal obligation, research, or marketing. Users should also be given the option to withdraw consent for the use of their data, particularly for marketing.

	Criteria	Criteria Origin
2b — Q1	Does the developer fully inform the user of how they will collect data about them?	ORCHA

	Criteria	Criteria Origin
2b — Q2	Does the developer provide users with details on all the purposes of processing user data?	ORCHA
2b — Q3	What is automatically shared data used for?	ORCHA
2b — Q4	Does the developer appear to intend to share or process the user data collected by the application for any purposes that have not been made clear to the user, or for any purposes they deem necessary?	ORCHA
2b — Q5	Does the developer inform users that they would like to use their data for the purpose of marketing?	ORCHA
2b — Q6	Does the developer obtain informed consent separately for the purpose of marketing?	ORCHA
2b — Q7	Is the user informed of how they can opt out of each processing activity?	ORCHA
2b — Q8	If the user cannot opt out of all processing activities, does the developer clearly explain which activities they cannot opt out of and why?	ORCHA
2b — Q9	Is the user informed that their data will not be shared with other parties, except for the purposes that have been set out in the privacy policy?	ORCHA

2c. Data storage and transit/transfer

Privacy policy related to data storage and data transfer should inform the user where their data is stored, how their data is protected in storage, and how it is protected in transit between the user's device and the host storage. The standards look for specific and secure storage techniques, such as industry-recognized encryption or firewalls.

	Criteria	Criteria Origin
2c — Q1	Does the data privacy policy or equivalent provide detail about where the data collected by the application will be stored (i.e., on the application or in an external data warehouse, cloud server, etc.)?	ORCHA

	Criteria	Criteria Origin
2c — Q2	Where is the data stored?	ORCHA
2c — Q3	Is the data stored in Canada? **Guidance:** This is an information provision criterion. That means this information can be displayed to end-users, so they can decide whether they would like to download an app that does not store their data in Canada.	MHCC
2c — Q4	Does the data privacy policy, or equivalent, state whether personal data is stored using industry-recognized secure data storage technologies?	ORCHA
2c — Q5	Is all personally identifiable data encrypted in transit between the device and any external host storage using industry-recognized methods?	ORCHA
2c — Q6	Is the user informed that online video consultations use secure industry standard encryption methods?	ORCHA

2d. Data standards and management

The standards will award additional points if an application developer is compliant with any international data management standards such as ISO 27001. The privacy policy should inform users of a data retention period and a method for data destruction. The standards also identify whether the developer has a policy in place to deal with any data security breaches.

	Criteria	Criteria Origin
2d — Q1	Does the policy state its compliance with recognized data management standards?	US DHAF
2d — Q2	Does the policy contain details of the length of time data is retained?	ORCHA
2d — Q3	Is there a statement containing details of a method for data destruction?	ORCHA

	Criteria	Criteria Origin
2d — Q4	Is there a statement that sets out a process for managing data confidentiality breaches? **Guidance:** The developer's privacy policy must provide details on the actions users should take and who they should contact in the event of a breach.	ORCHA
2d — Q5	Is there a statement that sets out the developer's processes/procedures for keeping an audit trail of access to PHI?	US DHAF

2e. GDPR/PPIPEDA/Privacy act/jurisdictional principles

This area focuses on the *General Data Protection Regulation* (GDPR), which in May 2018 came into force to replace the *Data Protection Act 1998*. The standards are concerned that all apps, particularly those developed in the U.K. and the EU, are fully compliant with the GDPR. This means providing a clear and explicit statement of compliance and confirming that the user is entitled to its seven user rights. This framework addresses the eighth user right — the right to be informed — in the questions under Data and Privacy Standards.

The developer should also inform the user about how they can exercise these rights and commit to responding within two months or less. Under the GDPR, the policy should outline the legal basis for the collection of user data and ensure that only minimal data is collected from the user.

Similar and additional requirements and user rights are observed under PIPEDA and have been built to specifically adapt this section to the MHCC's application standards.

All criteria relating to this section will only be asked for apps that collect and process personal and/or sensitive data and are therefore subject to PIPEDA or other provincial and territorial privacy laws deemed substantially *similar to PIPEDA.*

	Criteria	Criteria Origin
2e — Q1	Is there a statement that confirms the application's compliance with federal and/or provincial laws and regulations in the region in which it is being applied?	MHCC

	Criteria	Criteria Origin
2e — Q2	Is the user informed of the legal basis for which data is collected from them?	ORCHA
2e — Q3	What is the legal basis?	MHCC
2e — Q4	Is the user informed that the developer will only collect minimum data items that are necessary to provide their services, therefore ensuring that data minimization principles are met?	ORCHA
2e — Q5	Does the policy describe the processes the developer has in place to ensure that information is correct, complete, and current?	MHCC
2e — Q6	Is all user data processed in Canada?	MHCC
2e — Q7	Are users informed of international transfers?	MHCC
2e — Q8	Are users informed that while their data is being processed in another jurisdiction it may be accessed by courts, law enforcement, and national security authorities of that jurisdiction?	MHCC
2e — Q9	Is there a statement that the policy will be updated should the purpose of data collection change? This may mean reobtaining consent (if consent was the lawful basis).	ORCHA
2e — Q10	Are users informed of their rights with regards to their data?	ORCHA
2e — Q11	Has the developer made clear the existence of the data subject's right to request that their personal data be deleted?	ORCHA
2e — Q12	Has the developer made clear the existence of the data subject's right to access their personal data?	ORCHA
2e — Q13	Has the developer made clear the existence of the data subject's right to inspect their personal data?	US DHAF
2e — Q14	Is the user informed of their rights to know how their PHI is used and or shared?	US DHAF
2e — Q15	Has the developer made clear the existence of the data subject's rights to rectify their personal data?	ORCHA
2e — Q16	Has the developer made clear the existence of the data subject's rights to restrict the use of their personal data?	ORCHA

	Criteria	Criteria Origin
2e — Q17	Has the developer made clear the existence of the data subject's rights to object to the processing of their personal data?	ORCHA
2e — Q18	Has the developer made clear the existence of the data subject's rights to portability of their personal data?	ORCHA
2e — Q19	Has the developer made clear the existence of the data subject's right to withdraw consent for the use of their personal data?	ORCHA
2e — Q20	Has the developer informed the data subjects that they may exercise their rights under applicable laws and regulations?	US DHAF／MHCC
2e — Q21	Has the developer provided the user with information regarding the process for exercising said rights?	MHCC
2e — Q22	Has the developer made clear the existence of the user's right to request that they are not subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning them or similarly significant effects on them?	ORCHA
2e — Q23	Is the user informed of their right to challenge the organization's compliance with the fair information principles of PIPEDA?	MHCC
2e — Q24	Does the developer provide details through which the user can contact them to exercise their rights?	ORCHA
2e — Q25	Is the user informed of the time frame in which the developer will respond to any requests to exercise their rights?	ORCHA
2e — Q26	Is the user informed of any charges that might be incurred with regards to exercising their rights to access their personally identifiable information (PII)?	US DHAF
2e — Q27	Is the user informed of their right to have an access denial reviewed?	US DHAF

2f. Other data criteria

This subsection concerns children's data use (if applicable), or whether a user can report knowledge of a child accessing the apps without parental consent. The Office of the Privacy Commissioner of Canada refers to persons under 13 as *children*, those ages 13 to 18 as *youth*, and those 19 or older as *adults*. Because youth are considered old enough to make

their own decisions about their data, additional criteria surrounding the processing of children's data only apply to those under 13. The transparency of the privacy policy should extend to inform the user that any links to third-party websites or apps are not covered by the developer's privacy policy, and that users should make themselves aware of such third-party policies. In addition, the privacy policy should contain contact details that enable the user to make further enquiries regarding their data. The standards also explore whether the application provides the user with an additional, optional layer of security to protect their data.

	Criteria	Criteria Origin
2f — Q1	Are users clearly informed of the use of cookies when first landing on the developer's site/app?	ORCHA
2f — Q2	Are user's required to confirm their acceptance of the developer's use of cookies, when initially informed of their use?	ORCHA
2f — Q3	Does the developer address their use of cookies and collected data in their privacy policy or a separate cookie policy?	US DHAF
2f — Q4	Are users made aware of the use of strictly necessary cookies?	ORCHA
2f — Q5	Is user consent obtained for the use of non-strictly necessary cookies?	ORCHA
2f — Q6	Does the app save the user's cookie preferences?	MHCC
2f — Q7	Are users informed of how they can easily opt out of the use of cookies?	ORCHA
2f — Q8	Is the product aimed at children or likely to be used by children?	MHCC
2f — Q9	Is the application *particularly likely* to be used by children, even if they are not the primary market for the product?	ORCHA
2f — Q10	If the product is to be used by children, what age group is the product targeted at?	MHCC
2f — Q11	Are users informed of how they can report to the developer any knowledge of a child accessing the application and providing personal data without parental consent?	ORCHA
2f — Q12	Has a process been designed and put in place that allows children to easily access, understand, and exercise their own data protection rights?	ORCHA

	Criteria	Criteria Origin
2f — Q13	Where the legal basis for processing data was consent at the time the individual was a child, are requests for the erasure of data complied with whenever possible?	ORCHA
2f — Q14	Have children been consulted when designing this processing practice?	ORCHA
2f — Q15	Has the privacy policy been written in plain, age-appropriate language?	MHCC
2f — Q16	Is consent sought from a responsible parent/guardian?	ORCHA
2f — Q17	Does the policy specify that the developer will re-obtain parental consent should the information collected materially change, the purpose for which the information is processed changes, or the information is offered to new/different third parties?	US DHAF
2f — Q18	Does the developer ensure that parents are able to separately consent to their own internal use of the child's personal information, without having to consent to the disclosure of personal information to third parties?	US DHAF
2f — Q19	Are parents given the option to review the personal information collected from their children?	US DHAF
2f — Q20	Does the developer have a process for verifying the identity of the requester before responding to a request?	US DHAF
2f — Q21	Are parents given the option to revoke consent for the collection and processing of their children's personal information?	US DHAF
2f — Q22	Are parents given the option to request that the information collected from their children be deleted?	US DHAF
2f — Q23	Does the developer ensure that they do not seek parental/guardian consent when providing online preventive or counselling services to children?	ORCHA
2f — Q24	Are there two separate versions of privacy policies, one aimed at the child and the other at the responsible parent/guardian?	ORCHA
2f — Q25	When marketing the product outside of their country of residence, has the developer taken into consideration other jurisdictional laws regarding children's privacy (e.g., age restrictions)?	ORCHA

	Criteria	Criteria Origin
2f — Q26	Does the policy specify the types of personal data that will be collected from children?	US DHAF
2f — Q27	Does the policy specify how the developer will use the personal data collected from children?	US DHAF
2f — Q28	Does the policy specify whether such personal data will be shared with advertisers or other third parties?	US DHAF
2f — Q29	Is the user made aware that by following links to third-party websites, the developer's policies no longer apply, and that the user should make themselves aware of the third party's policies?	ORCHA
2f — Q30	Is the user informed of how they can make further inquiries about the company's privacy policy?	ORCHA
2f — Q31	Does the application allow the user to set their preferences for sharing the application data with or from other apps (e.g., Facebook/Instagram/Fitbit)?	ORCHA
2f — Q32	Is there functionality within the application to allows the user to set their preferences for sharing application data with other users (e.g., clinicians, carers, family, friends)?	ORCHA
2f — Q33	Is it strictly necessary for anyone to easily access the personal information that persists on the device (e.g., to access health information during an emergency)?	ORCHA
2f — Q34	Are users provided options to introduce additional security measures to protect their data on the app (e.g., set additional pass codes for access to the app, after accessing the device is unlocked)?	ORCHA
2f — Q35	Does the application use a sign-up/sign-in verification/authentication model?	ORCHA
2f — Q36	What type of model is being used? (Please describe.)	ORCHA
2f — Q37	Do any of the following types of dark pattern appear in the app? (Please select those that appear.)	MHCC

3. Clinical Evidence Standards

3a. Evidence of effectiveness

Where effectiveness claims are not made directly by the developer, the necessity of evidence needs to be considered, both in relation to the app's claimed or implied benefits and to the risk of harm associated with its use. As was highlighted in the App Overview, proportionality of evidence/assurance evidence can initially be evaluated before an assessment of necessity, appropriateness, and quality.

Proportionality must be considered because it is unrealistic to expect all apps to provide the same types of evidence. ORCHA's Adapted Evidence Standards Framework (adapted ESF) guards the functional complexity of the app and the risk of harm to users while guiding the evidence requirement. For example, a higher level of evidence is called for with apps that have more complex functionality, since they harbour higher risks (see subsection 3d). Those that lack this evidential requirement may be able to provide alternative credentials to pass the professional assurance standard. This is considered on a case-by-case basis. Subsection 3d also provides more information on alternative credentials.

Necessity focuses on whether evidence of effectiveness is reasonably required in the first place and whether this requirement places a disproportionately unfair burden on developers, compared to non-digital (similar) solutions. An example would be an app that provides a diary for those with depression/anxiety to write down their thoughts. In such a case, a question needs to be asked as to whether a similar notebook bought from the local store would require such evidence. If the adapted ESF indicates, "Yes, the app needs to provide evidence because there is a potential added risk associated with its use," it then becomes necessary to determine which type of evidence is required: evidence of effectiveness, evidence of safety, or both. For instance:

- **Safety scenario**. If an app makes use of an established clinical calculator, it may provide indirect evidence that shows the safety of a specific calculation or algorithm but not in the specific context of the app. In this instance we would look for assurance that the app has accurately replicated the relevant algorithm and that it functions and produces outputs in an identical way that does not result in misinterpretations.
- **Effectiveness scenario I.** If an app claims or implies a specific benefit, as highlighted in App Overview, we would require evidence of effectiveness to support its claimed or implied benefit.
- **Effectiveness scenario II**. If an app directs readers to indirect evidence to support claimed/implied benefits, this can be considered sufficient if the mode and function of the app is identical in all material ways to the solution identified in the indirect evidence (see subsection 3b).

Appropriateness is determined by whether any investigations or research concerning the effectiveness or safety of an app has been conducted using a representative sample group and using appropriate evaluation methods. For instance, mandating a randomized controlled trial (RCT) for diagnostics would not intuitively make sense. The target audience of the app is identified in the app overview, and the evidence must show that it has selected a sample group with the same key characteristics (e.g., age range, gender). If the evidence is not conducted using an appropriate sample group, or an appropriate means of evaluation, then its quality cannot be assessed.

Appropriateness can also be assessed for apps that do not require evidence, but rather assurance; i.e., those associated with a much lower risk profile (typically NICE ESF Tier 2b or lower). The assessor would research whether any clinicians were involved in the app's development and whether they held appropriate qualifications. The appropriateness of any statements, referenced guidelines, and relevant information can also be assessed at this point.

Quality also relates to whether evidence or assurance is deemed appropriate. If the app needs to provide evidence of effectiveness, and this threshold for the appropriate type of evidence has been met, then the quality of that evidence can be assessed. For example:

- In the case of digital therapeutics, quality is considered through the evaluation of significant p values ($p < 0.05$) and comparators/validated comparators (as outlined in the criteria below).
- In the case of diagnostics, identification of either improvements or non-significant reductions in diagnostic accuracy in terms of confidence-interval overlapping and AUROC (sensitivity and specificity criteria) are also used.

Though these are the most widely used quality indicators, quality is assessed on a case-by-case basis to make sure it is proportional to what the app is doing/looking for.

As mentioned, when evidence of diagnostics and treatments are considered, p values of < 0.05 can be inappropriate. Evidence here is taken on a case-by-case basis, but regular themes that demonstrate safety include high levels of sensitivity/specificity or similar levels of adherence to the expertise of a qualified clinician.

	Criteria	Criteria Origin
3a — Q1	What type(s) of evidence is available?	ORCHA
3a — Q2	Provide links to the publicly available evidence/published evidence that the developer has provided.	ORCHA
3a — Q3	For each type of relevant evidence — • What category does the evidence relate to?	ORCHA

	Criteria	Criteria Origin
3a — Q4	For each type of relevant evidence — • What benefit does the evidence relate to?	ORCHA
3a — Q5i	For each type of relevant evidence — • What is the sample size?	MHCC
3a — Q5ii	• Does the sample reflect the app's target audience, as stated by the developer?	MHCC
3a — Q6	For each type of relevant evidence — • Does the evidence found provide a p value?	ORCHA
3a — Q7	For each type of relevant evidence — • Does the p value demonstrate significance ($p < 0.05$)?	ORCHA
3a — Q8	For each type of relevant evidence — • Does the p value demonstrate near significance ($p < 0.2$)?	ORCHA
3a — Q9	For each type of relevant evidence — • Is there a comparator?	ORCHA
3a — Q10	For each type of relevant evidence — • Is the comparator validated?	ORCHA

3b. Behavioural change

If an application uses accepted behaviour change techniques that already have a strong evidence base, the developer may choose not to fund additional research. For example, if an application incorporated dialectic behaviour therapy (a behaviour change technique), the developer may choose to refer to its strong evidence base instead of conducting their own research.

	Criteria	Criteria Origin
3b — Q1	Does the application have its own high-quality study?	ORCHA
3b — Q2	Does the application reference and evidence its behaviour change technique?	ORCHA

3c. Professional backing

Professional backing refers to evidence that an appropriate professional was involved in an application's design and development. The relevant professional will differ depending on the context. For example, for a simple meditation application, a qualified meditation instructor would be accepted as an appropriate professional. For a complex clinical solution such as an application that claims to treat depression, a relevant qualified clinician would be necessary.

Professional backing can be inferred if the application has been externally accredited. External accreditations are wide ranging, from national health bodies to charities. Like the appropriate professional role, it is essential that the accreditation come from an appropriate body that is relevant to the application. Note: while the criteria below relate to professional assurance, Q9-Q14 also strongly focus on the developer's efforts to ensure that the app is safe.

	Criteria	Criteria Origin
3c — Q1	Is there a suitably qualified professional involved in the application's development team?	ORCHA
3c — Q2	Please provide the licensed health care professionals involved in the delivery of the app. **Guidance:** This question applies only if a health-care professional is involved in the delivery of the app as identified through 1h — Q5.	MHCC
3c — Q3	Does the organization behind the application have relevant credentials?	ORCHA
3c — Q4	Is there evidence of an endorsement by a relevant body?	ORCHA
3c — Q5	Are organizations using the app?	ORCHA
3c — Q6	What type of organization is using the app?	MHCC
3c — Q7	Is there a statement that the app has been positively evaluated or validated by a relevant health-care professional?	ORCHA
3c — Q8	Please specify who the relevant experts are and what qualifications they hold.	ORCHA

	Criteria	Criteria Origin
3c — Q9	Is there evidence within the application that the developer has validated any guidance with relevant reliable information sources or references?	ORCHA
3c — Q10	Is there a statement or any evidence showing that appropriate safeguarding measures are in place around peer support and other communication functions within the platform? • (Tier 2a requirement: only asked of apps that require such measures because of its functional capabilities/intended purpose)	ORCHA
3c — Q11	Does the application offer 24-7 peer or clinical support? **Guidance:** The support can be offered via chat/consultation on demand or another 24-7 resource(s). This question only applies to apps that discuss suicidal ideation or meet Tier 2b and above criteria (from the ESF Tiers).	MHCC
3c — Q12	Does the developer clearly identify who the application should and should not be used by?	ORCHA
3c — Q13	Does the developer publish their risk management processes?	ORCHA
3c — Q14	Does the developer make clear risks associated with using the app?	ORCHA
3c — Q15	Is there a way for the user to confirm that the data input is accurate?	ORCHA

3c — Q16	Does the app direct users to a government website (provincial/territorial/federal)?
	Relevant federal examples:
	• English —
	  ○ Mental Health Support: Get Help
	  ○ Substance Use
	• French —
	  ○ Soutien en santé mentale : Demander de l'aide
	  ○ Consommation de substances
		MHCC

	Criteria	Criteria Origin
	Guidance: This question only applies if the app does not provide a chat/ consultation on demand or another 24-7 resource(s).	

3d. ORCHA Adapted Evidence Standards Framework compliance

Every app is expected to provide some level of evidence or assurance. It was agreed that this level of evidence and assurance should remain proportional to the app's functionality and claims.

The framework makes use of ORCHA's Adapted Evidence Standards Framework (adapted ESF), which amended the original NICE ESF so that the requirements were fair to mobile health applications.

The adapted ESF works by giving each app an "ESF Tier" based on its functionality. The adapted ESF Tier then determines what level of evidence should be provided. Passing its tier requirement by meeting its level of evidence and assurance would positively impact the app's review.

An application's ESF Tier is determined by what it offers.

The app would be classified as Tier 3b if it does one of the following:

- Diagnoses a mental health problem (1e-Q2 is yes)
- Contains a novel clinical calculator that impacts care, treatment, or diagnosis (1e-Q11 is yes)
- Automatically measures and/or records data about a user's specified mental health problem and transmits the data to a professional, carer, or third-party organization, without any input from the user (1g-Q7 is yes)
- Provides treatment (1e-Q15 is yes)
- Guides the treatment of a mental health problem (1e-Q17 is yes)
- Alleviates the symptoms of an existing mental health problem (1e-Q25 is yes)

An app would be classified as Tier 3a if it does none of the things listed above but does one of the following:

- Serves as a complex self-management app (selected in 1g-Q4)
- Includes preventive behaviour change within the app (selected in 1g-Q10)

- Has a recognized (not novel) clinical calculator within the app (1e-Q11 is yes and 1e-Q12 mentions an established clinical calculator)

Wysa is a mental health support application that provides a chatbot for users to discuss anything from sleep to stress. It is a complex self-management application that would place it under Tier 3a or 3b, depending on further functionalities. It also enables users to assess themselves symptomatically based on depression tests like PHQ-9 and anxiety tests like GAD-7. These would be considered clinical calculators, but since they are widely recognized and established resources the application would not be increased to Tier 3b. This app remains at Tier 3a due to its complex management and specific use related to a mental health problem.

An application containing a novel clinical calculator that is unique would not be an established tool and likely not have as much recognition or reference. This type of application would therefore be subject to more rigour and would be considered Tier 3b.

An app would be designated Tier 2b if it does none of the things listed in the 3b/3a tiers and is classified as a standard self-management application (selected in 1g-Q4).

An application would be classified as Tier 2a if it does none of the things listed in the 3b/3a/2b tiers and does one of the following:

- Provides information or guidance (1d-Q1 is yes) or allows a health-care professional to provide clinical advice, as opposed to the app providing it (1g-Q3 is yes)
- Provides information, resources, or activities to the public, users, or clinicians, either about a specific mental health problem or general health and lifestyle (1d-Q5 is yes)
- Provides two-way communication between users, citizens, or health-care professionals (1l-Q4 is yes) or is a simple self-management app (selected in 1g-Q4)

Moodbeam is an application that helps users keep track of how they are feeling. It has two simple buttons to represent when the user feels a high and when they feel a low, and this information can then be explored as patterns and trends over time. This application is a good example of *simple* self-management, which is classified as Tier 2a.

A simple self-management application allows users to monitor their non-specific mental health-problem data, which can then be displayed back to them in a simple format. Since Moodbeam enables users to monitor their mood and feelings and see their data in a simple graph form, it is considered simple self-management and therefore appropriate for Tier 2a.

If this application allowed users to monitor data that was specific to a mental health problem, such as reporting when they felt clinical depression or generalized anxiety, then it would no longer fit into Tier 2a. When an application is able to monitor specific mental health problem data and display it back to the user in simple graph form, it is considered *standard* self-management and therefore appropriate for Tier 2b.

An application would be considered Tier 1 if it does none of the things listed in the 3b/3a/2b/2a tiers and provides no user outcomes. For example, it may act as an administrative application that helps deliver health-related systems/services, or it could work as a maintenance application to report and fix issues around a hospital.

Thalamos is a web application that helps health-care professionals complete and manage forms for use under the U.K.'s *Mental Health Act*. It is a good Tier 1 example because it simply replaces pen and paper. Since the application facilitates administration and has no direct impact on user outcomes, it could not be classified any higher than Tier 1.

Once an app has been assessed for its ESF Tier classification, the next aim is to understand whether it is compliant with that tier. Doing so requires that the relevant flagged criteria are met by positive answers.

Here, it is important to note that requirements are cumulative, meaning that an app at 3a must meet requirements at a lower tier. However, if the app has an RCT, which is acceptable at tier 3b, there is no requirement for a separate observational study. One study (an RCT) would be enough in that case.

The app would have met Tier 1 minimum requirements if it has

- evidence of a survey, pilot study, meta-analysis, RCT, observational, or other indicated user acceptance/benefit (3a-Q1 does not contain none)

and at least one of the following:

- evidence of a relevant professional involved in the development team (3c-Q1 is yes)
- relevant organizational credentials (3c-Q2 is yes)
- evidence of endorsement by a relevant body (3c-Q3 is yes).

The app would have met Tier 2a minimum requirements if it has

- evidence that the developer has validated the information, advice, or guidance with relevant and appropriate academic studies or relevant academic expert input (3c-Q1 or 3c-Q2 or 3c-Q7 is yes).
- there is clear evidence of safeguarding measures being in place for any communication functions (4b-Q1 is yes, if applicable)
- the app has evidence of accrediting expertise (3c-Q1 or 3c-Q2 or 3c-Q3 or 3c-Q5 is yes).

The app would have met Tier 2b minimum requirements if it has

- evidence that the developer has validated the information, advice, or guidance (3c-Q1 or 3c-Q7 is yes)
- clear evidence of safeguarding measures being in place for any communication functions (4b-Q1 is yes, if applicable)
- evidence of accrediting expertise (3c-Q1 or 3c-Q2 or 3c-Q5 is yes)

- evidence of an endorsement by a relevant body (3c-Q3 is yes) or a meta-analysis, or an observational study/RCT with a *p* value < 0.05 (3a-Q1 is a yes, and one of the 3a-Q7 answers is a yes).

The app would have met Tier 3a minimum requirements if it has

- evidence of an RCT (3a-Q1 answer includes RCT) that has a significant *p* value (3a-Q7 is yes) or evidence of an observational study (3a-Q1 answer includes observational) that has a significant *p* value (3a-Q7 is yes)
- a comparator (3a-Q9 is yes) or a validated comparator (3a-Q10 is yes).

The app would have met Tier 3b minimum requirements if it has

- evidence of an RCT (3a-Q1 answer includes RCT) that has a significant *p* value (3a-Q7 is yes)
- a validated comparator (3a-Q10 is yes).

If an app has been classified as a Tier 3b but does not have an RCT, it could still pass the ESF using alternative credentials. While each app would be considered on a case-by-case basis, Tier 3b can be met by providing quality real-world evidence. For example:

- high-quality observational studies instead of RCTs
- evidence of adoption and use

	Criteria	Criteria Origin
3d — Q1	What tier of the ESF is the app?	ORCHA
3d — Q2	Is the application Tier 1?	ORCHA
3d — Q3	Is the application Tier 2a?	ORCHA
3d — Q4	Is the application Tier 2b?	ORCHA
3d — Q5	Is the application Tier 3a?	ORCHA
3d — Q6	Is the application Tier 3b?	ORCHA
3d — Q7	Has the application met Tier 1 requirements?	ORCHA
3d — Q8	Has the application met Tier 2a requirements?	ORCHA
3d — Q9	Has the application met Tier 2b requirements?	ORCHA
3d — Q10	Has the application met Tier 3a requirements?	ORCHA
3d — Q11	Has the application met Tier 3b requirements?	ORCHA

	Criteria	Criteria Origin
3d — Q12	Does the application have appropriate evidence for the ESF Tier?	ORCHA

3e. Other Areas of interest

	Criteria	Criteria Origin
3e — Q1	Does the sample of the research study meet the relevant characteristics for the users of the app?	MHCC

4. Clinical Safety Standards

4a. Software as a medical device

The functionality of any software product, and the ways it is represented or labelled for use, dictates whether it qualifies as a medical device under the Canadian *Food and Drugs Act* and the *Medical Devices Regulations*, administered by Health Canada.

Software that has no direct impact on the diagnosis, treatment, or management of an individual's disease, disorder, abnormal physical state, or symptoms would not be subject to the *Medical Devices Regulations*. Health Canada's Software as a Medical Device (SaMD) guidance document can assist manufacturers in determining whether their product is a medical device.

If a software product is identified as a medical device, its risk classification must also be determined to know which regulatory requirements apply. (Medical devices are classified under four classes, with Class I representing the lowest risk and Class IV the highest.) For example, to be sold in Canada, Class I devices do not require a medical device licence, whereas Class II, III, and IV devices do require one (Note: Class I manufacturers, importers, or distributors also have regulatory requirements).

Many mental health apps perform functions that would potentially bring them under the *Medical Devices Regulations* in Canada. These functions include apps that could help treat, alleviate, diagnose, or prevent mental health-related symptoms. These parameters could impact many of the leading apps in this area, and excluding them from this framework would severely limit its reach.

The approach typically adopted in jurisdictions such as the U.K. and the EU is to ensure that the applicable framework can identify whether or not an app is a medical device under the relevant local regulations, and if it is, to validate whether or not it has been appropriately certified or authorized under those regulations.

This approach is not about bypassing the relevant certification/authorization process. It simply seeks to validate whether that process has already been completed through the establishment of an appropriate mark, certificate, or authorization (i.e., in the Canadian context, a medical device licence).

This is the approach we are proposing for the current assessment framework. Such a strategy would allow apps to be potentially classified as medical devices and would also enable us to identify any without suitable authorization. Any apps deemed to be medical devices without Health Canada authorization would be rejected from the framework process and referred to Health Canada for resolution.

The only other practical route to avoid the risk of inadvertently including unauthorized medical devices in the framework process would be to explicitly exclude apps with relevant functionality from the start. As noted, however, this would severely limit the types of products that could be assessed via the framework. The proposed step-by-step process we would follow if we allow relevant apps into the process (including the criteria) would be as follows:

If the mental health app has a "medical purpose," it is subject to the *Medical Devices Regulations* and requires appropriate regulatory authorization from Health Canada. To determine whether regulatory authorization is required, the following criteria are to be met:

	Criteria	Criteria Origin
4a — Q1	Is the application a medical device that is subject to the *Medical Devices Regulations* according to Health Canada's Software as a Medical Device guidance document? If 4a-Q1 is answered no (the application is not intended for one or more medical purposes), then Q2 does not need to be answered.	ORCHA
4a — Q2	If the application fits the criteria for a Class II medical device or higher, is the application authorized for sale in Canada? • Health Canada's Medical Devices Active Licence Listing (MDALL) can be consulted to determine whether a product has an active licence.	MHCC

	Criteria	Criteria Origin
	• A medical device establishment licence[6] (MDEL) is required for Class I manufacturers, importers, or distributors. It is not product-specific, nor does it represent any product-specific assessment by Health Canada.	

Please note the following:

- Health Canada does not maintain a list of products (e.g., specific medical devices) under an MDEL.
- An MDEL does not constitute approval of any specific medical devices imported or distributed by the MDEL holder.

If it appears that the app is subject to the *Medical Devices Regulations* (i.e., it is a medical device) but has not been authorized by Health Canada, any advertisement, sale, or distribution of the app in Canada would be prohibited. In such cases, the app manufacturer could contact Health Canada's Medical Devices Directorate.

4b. Safety/Risk management

Developers should consider the risks that come with making a mental health app to ensure that it can be used safely. Because Canada has no formal standards to guide developers in creating safe mental health apps, this framework proposes that they adopt the ORCHA Clinical Safety Assessment (OCSA), whose criteria objectively outline safety considerations app developers could adhere to. Apps that comply with the ISO 14971 (a framework for risk management) and DCB 0129 (a clinical risk management framework) would also pass the OCSA standards. Not only is the OCSA is aligned with the established risk management frameworks for health apps, its criteria have been tailored to the Canadian context (as shown in the criteria below).

	Criteria	Criteria Origin
4b — Q1	Is the app/solution in scope of the ORCHA Clinical Safety Assessment (OCSA)?	ORCHA
4b — Q2	Why is the application in scope?	ORCHA

[6] A medical device establishment licence is issued to Class I manufacturers as well as importers or distributors of all device classes to permit them to import or distribute a medical device in Canada. An MDEL provides Health Canada assurance that procedures are in place to protect the public should a problem with a device be identified.

	Criteria	Criteria Origin
4b — Q3	Has the developer provided a *thorough* summary about why the application is out of scope (e.g., it is complete and matches the functionality put forward)?	ORCHA
4b — Q4	What risks, if any, have been documented concerning harm to a user?	ORCHA
4b — Q5	If the application/solution was deemed to be in scope, has the developer supplied suitable risk management documentation?	ORCHA
4b — Q6	Is there risk management documentation?	ORCHA
4b — Q7	Does the developer outline the need for risk management documentation?	ORCHA
4b — Q8	Does the risk management documentation have a full version history and issue date published?	ORCHA
4b — Q9	Has the developer described their clinical risk management system (e.g., identification of key personnel, their roles and responsibilities, identification of clinical risk management governance structure)?	ORCHA
4b — Q10	Does the safety case mention a test summary (i.e., a summary of any outstanding test issues and their impact on clinical safety)?	ORCHA
4b — Q11	Does the hazard log have a full version history and issue date published?	ORCHA
4b — Q12	Are the hazards listed complete? **Guidance:** From a review of the hazards listed, have all the required details been completed, such as name, clinical impact, and risk ratings?	ORCHA
4b — Q13	Are the potential harms related to the user?	ORCHA
4b — Q14	Do the harms outline what the clinical impact may be for the user?	ORCHA
4b — Q15	Has the developer covered all of the possible causes for each hazard?	ORCHA
4b — Q16	Do the risk ratings look appropriate or do they appear to be “copy and paste” throughout the listed hazards?	ORCHA
4b — Q17	Are hazards split incorrectly into potential and actual harm?	ORCHA

	Criteria	Criteria Origin
4b — Q18	Has the developer implemented the clinical risk analysis activities defined in the clinical risk management plan?	ORCHA
4b — Q19	Is the clinical risk analysis carried out by a multidisciplinary group?	ORCHA
4b — Q20	Has the developer defined the clinical scope of the health IT system to be delivered?	ORCHA
4b — Q21	Has the developer defined the intended use of the health IT system to be delivered?	ORCHA
4b — Q22	Does the risk management documentation make clear where the application fits into the clinical workflow?	ORCHA
4b — Q23	Has the developer outlined third-party products integrated within the health IT system to be released?	ORCHA
4b — Q24	Has the developer deploying the health IT system considered how it will impact current business processes and ways of working?	ORCHA
4b — Q25	Is there usability- and human-factor-related evidence within the scope?	ORCHA
4b — Q26	Has the developer assessed any infrastructure at the health organization within their scope of influence that is required to support the deployment of the health IT system? (This may be achieved by the manufacturer specifying the minimum system requirements.)	ORCHA
4b — Q27	Is the developer undertaking any data migration? (Where data migration is to be undertaken by the developer, it should be included in the scope of the clinical risk management activities.)	ORCHA
4b — Q28	Is the data migration being undertaken by the developer properly covered in the documentation?	ORCHA
4b — Q29	Has the developer identified any hazards associated with the data migration that has been analyzed and suitably mitigated (working in conjunction with the relevant health organization, as appropriate)?	ORCHA
4b — Q30	Has the developer considered the end-to-end clinical process, including functionality and how that functionality is used?	ORCHA

	Criteria	Criteria Origin
4b — Q31	Has the developer considered inter- and intra-health IT system messaging?	ORCHA
4b — Q32	Has the developer assessed the health IT system's architecture and design?	ORCHA
4b — Q33	Is a clear matrix used to define the risk ratings?	ORCHA
4b — Q34	For each identified hazard, has the developer evaluated whether the initial clinical risk is acceptable?	ORCHA
4b — Q35	Has the developer used the risk acceptability criteria that was previously defined?	ORCHA
4b — Q36	Has the developer identified appropriate clinical risk control measures to remove any unacceptable clinical risk?	ORCHA
4b — Q37	Has the developer assessed proposed clinical risk control measures to determine whether new hazards will be introduced as a result of the measures?	ORCHA
4b — Q38	Has the developer assessed proposed clinical risk control measures to determine whether the clinical risks for previously identified hazards will be affected?	ORCHA
4b — Q39	Is the developer managing new hazards or increased clinical risks?	ORCHA
4b — Q40	For each identified hazard, has the developer evaluated whether the residual clinical risk is acceptable?	ORCHA
4b — Q41	Has the developer used the risk acceptability criteria previously defined?	ORCHA
4b — Q42	If the residual clinical risk is unacceptable, has the developer identified additional clinical risk control measures to reduce the clinical risk?	ORCHA
4b — Q43	If the developer has determined that no suitable risk control measures are possible, have they conducted a clinical risk benefit analysis?	ORCHA
4b — Q44	Has the developer's analysis shown that the clinical benefits of the intended use outweigh the residual clinical risk?	ORCHA

	Criteria	Criteria Origin
4b — Q45	Has the developer implemented the identified clinical risk control measures (except where these are to be implemented by another organization)?	ORCHA
4b — Q46	Have the clinical risks from all identified hazards been considered and accepted?	ORCHA
4b — Q47	Have any hazard rating reductions been fully justified?	ORCHA
4b — Q48	Is there a professional involved in the clinical safety process?	MHCC
4b — Q49	Is the relevant professional suitably qualified?	ORCHA
4b — Q50	Does the relevant professional have appropriate registration details?	ORCHA
4b — Q51	Have these registration details played an active part in the process?	ORCHA

5. Usability and Accessibility Standards

5a. Design and development

This section considers the design and development of the app, and whether it follows any recognized application design standards, such as WC3, WCAG 2.0 AA, WCAG 2.1 AA, ISO 9241, Apple HIG, or Android Application Quality Guidelines. The review also considers whether there was any user involvement during the development of the app, user involvement in testing, or if any features were based on user feedback.

	Criteria	Criteria Origin
5a — Q1	Is there a statement within the application outlining compliance with any currently recognized application design standards? • WC3 • WCAG 2.0 AA • WCAG 2.1 AA • ISO 9241	MHCC

	Criteria	Criteria Origin
	• Apple HIG • Android Application Quality Guidelines • ISO 25062 • MAUQ • ADA • AODA	
5a — Q2	Is there a statement about lived and living experience feedback during design/development? **Guidance:** This criterion is to determine if relevant feedback from those with lived and living experience had been considered in the design of the app, before or after the app was released.	ORCHA
5a — Q3	Was the app co-designed by one or more people with lived and living experience?	MHCC
5a — Q4	Is there a statement about lived and living experience feedback from a community organization/online community during design/development? **Guidance:** This criterion is to determine if relevant feedback from a community organization/online community from those with lived and living experience had been considered in the design of the app, before or after the app was released. This criterion follows 5a-Q2 to remove the risk of biased feedback and encourage developer's to reach out to communities.	MHCC
5a — Q5	Is there any evidence of lived and living experience involvement in testing?	MHCC
5a — Q6	Was user testing carried out with the relevant population the product has been designed for?	MHCC
5a — Q7	Has any user testing considered a diverse range of participants, with regards to differing cultures and demographics?	MHCC
5a — Q8	Has user testing considered participant differences in language?	MHCC
5a — Q9	Has user testing considered participant differences in gender?	MHCC

	Criteria	Criteria Origin
5a — Q10	Has user testing considered participant differences in sexual orientation?	MHCC
5a — Q11	Has user testing considered participant differences in race?	MHCC
5a — Q12	Has user testing considered participant differences in ethnicity?	MHCC
5a — Q13	Has user testing considered participant differences in religion?	MHCC
5a — Q14	Has user testing considered participant differences in spirituality?	MHCC
5a — Q15	Is there evidence of continuing to work with or include people with lived and living experience in the product's development?	MHCC
5a — Q16	Is the app continuously developed, supported, and maintained?	MHCC
5a — Q17	Has the developer detailed their approach to continuous development, including reviewing their feedback?	ORCHA
5a — Q18	Does the detailed approach include key evaluative measures and/or indicators?	MHCC
5a — Q19	Does the developer have a post-release schedule or indicate how frequently they look at the need for changes?	ORCHA
5a — Q20	Has the developer indicated their process for reviewing content to ensure that it is aligned with up-to-date clinical guidelines?	ORCHA

5b. Accessibility

Accessibility is important to consider, given that the application should be accessible to all users regardless of their specific needs. The review considers whether the application is customizable to suit certain needs, such as poor sight or hearing impairment. If the application uses any specialist or medical terms, these should be clearly explained to the user.

	Criteria	Criteria Origin
5b — Q1	Can the user change the font size in-app/does the application respond to device preferences?	ORCHA
5b — Q2	Does the application provide support for users with poor sight?	ORCHA

	Criteria	Criteria Origin
5b — Q3	Does the application provide support for users with hearing difficulty?	ORCHA
5b — Q4	Are there any components of the app which can be used to operate without Wi-Fi?	MHCC
5b — Q5	Is the app suitable for low-bandwidth connections?	MHCC

5c. Usability

Accessibility also relates to the usability of the app, including further customization options. The review identifies if the application has any functions to aid navigation, such as a home button, back button, help button, or search feature. If the application utilizes push or email notifications, the standards identify whether the user has options to manage these for their own preference or privacy, both at the application and device level. Finally, if there are any bugs identified, these will be flagged. If the application contains a forum, then we look for a statement to ensure that forum content is moderated.

	Criteria	Criteria Origin
5c — Q1	Can the user change the presentation theme such as language?	ORCHA
5c — Q2	Are any medical, specialist, or technical terms explained clearly to the user?	ORCHA
5c — Q3	Does the application send push notifications?	ORCHA
5c — Q4	Does the application send email notifications?	ORCHA
5c — Q5	Does the user have options to manage the notification settings (push/email) within the application for convenience/privacy?	ORCHA
5c — Q6	Does the application inform the user how to manage notification settings for convenience/privacy (to prevent information being shown if the device is locked but on show)?	ORCHA
5c — Q7	Was there any evidence of bugs during the review?	ORCHA

5d. Support

Support is a key area, since it is important that users know how to contact the developer if they have any problems or questions with the application. The standards also identify *what type of support* is offered to users, and if there is a commitment from the developer to respond to any user queries. We would expect to see that the type of support offered is appropriate to the application complexity; that is, a higher complexity application would require a more sophisticated offer of user support.

	Criteria	Criteria Origin
5d — Q1	If there is a forum, is there a statement within the application that the forum content is moderated?	ORCHA
5d — Q2	Is there a statement about how to report technical issues to the developer?	ORCHA
5d — Q3	What kind of support is offered? • email address • live chat/chatbot • eTicket • helpline/telephone number	ORCHA
5d — Q4	Can the user contact other users for peer support?	MHCC
5d — Q5	Does the application provide technical support, therapeutic support, or both?	MHCC
5d — Q6	If therapeutic support is provided, is the application transparent regarding who this is provided by?	MHCC
5d — Q7	If therapeutic support is provided, is there a commitment from the app developer in terms of a time scale for response?	MHCC
5d — Q8	Is there any statement within the application about the developer's commitment to addressing problems reported to them (e.g., time scales to respond, commitment to eradicate reported bugs and faults)?	ORCHA
5d — Q9	Is there a help feature accessible from every page of the app (e.g., an information button)?	MHCC
5d — Q10	Is there a clear, universally recognized help icon such as a question mark?	MHCC

	Criteria	Criteria Origin
5d – Q11	Does the app collect user feedback through an appropriate channel? **Guidance:** An appropriate channel requires a formalized process (reviews from the Apple App Store or Google Play Store would not suffice).	MHCC

6. Security and Technical Stability Standards

6a. Technical stability

	Criteria	Criteria Origin
6a — Q1	Does the application connect to an internet-based application programming interface (API) (e.g., an application developer web service, social media, advertisements)?	ORCHA
6a — Q2	List the APIs.	ORCHA
6a — Q3	Does the application integrate with a device?	ORCHA
6a — Q4	Does the application integrate with any of the following: electronic medical record (EMR), electronic health-care record (EHR), personal health record (PHR), or clinical specialty system (CSS)?	MHCC
6a — Q5	Does the application operate without Wi-Fi?	ORCHA
6a — Q6	Does the application operate without a cellular network?	ORCHA
6a — Q7	Does the application access, process, or store personal and/or sensitive data?	ORCHA
6a — Q8	Is sensitive data persisted[7] to the mobile device?	ORCHA

[7] Persistence enables data to continue after the process that created it has ended.

	Criteria	Criteria Origin
6a — Q9	Does the application access, process, or store personal and/or sensitive data?	ORCHA
6a — Q10	What permissions does the application request?	ORCHA
6a — Q11	Does the application provide alerts or notifications?	ORCHA
6a — Q12	Does the application provide suggestions?	ORCHA
6a — Q13	Does the application undertake calculations?	ORCHA
6a — Q14	Is the source code and any configuration items for the product version-controlled with all changes audited?	ORCHA
6a — Q15	• Provide details of any associated processes/procedures and tools that are used.	ORCHA
6a — Q16	Do you have the capacity to roll back to previous versions of your product?	ORCHA
6a — Q17	• Provide details of any associated processes/procedures and tools that are used.	ORCHA
6a — Q18	Describe your processes for accepting and responding to technical faults from end-users.	ORCHA
6a — Q19	Do you provide online support for user queries?	ORCHA
6a — Q20	Do you proactively monitor the running of systems and system components to automatically identify faults and technical issues?	ORCHA
6a — Q21	• Provide details of any associated processes/procedures and tools that are used.	ORCHA
6a — Q22	Do you have a documented roadmap for future development of your product?	ORCHA
6a — Q23	• Provide details of planned development, technical updates.	ORCHA
6a — Q24	Provide details of how you will ensure the continued availability of your product.	ORCHA
6a — Q25	Do you have a plan for decommissioning your product?	ORCHA
6a — Q26	Describe your processes for decommissioning your product and dealing with any identifiable data.	ORCHA

	Criteria	Criteria Origin
6a — Q27	Do you have a plan for dealing with any identifiable data in the event that an individual stops using your product (e.g., by uninstalling or unsubscribing)?	ORCHA
6a — Q28	• Provide details of any associated processes/procedures and tools that are used.	ORCHA
6a — Q29	Does the organization follow any formal testing standards?	ORCHA
6a — Q30	• Provide details of any associated processes/procedures and tools that are used.	ORCHA
6a — Q31	For each of the following that are carried out, please describe the people/roles involved and the processes they work on, even if they are informal.	ORCHA
6a — Q32	• unit	ORCHA
6a — Q33	• regression	ORCHA
6a — Q34	• end to end/integration	ORCHA
6a — Q35	• user acceptance	ORCHA
6a — Q36	A/B **Guidance:** A form of UX testing in which two variants of something (A and B) are tested to determine the better of the two variants.	ORCHA
6a — Q37	• PEN/vulnerability	ORCHA
6a — Q38	• testing across devices	ORCHA
6a — Q39	• load/performance	ORCHA
6a — Q40	• security	ORCHA
6a — Q41	• other non-functional tests	ORCHA
6a — Q42	• other testing	ORCHA

6b. Technical security

	Criteria	Criteria Origin
6b — Q1	Is the application a native application for a mobile device?	ORCHA
6b — Q2	Is the application a web application?	ORCHA
6b — Q3	Are web APIs accessed?	ORCHA
6b — Q4	Does the application access, process, or store personal and/or sensitive data?	ORCHA
6b — Q5	Is sensitive data persisted to the mobile device?	ORCHA
6b — Q6	What permissions does the application request?	ORCHA
6b — Q7	What OWASP level is the app categorized as? **Guidance:** The assessor should use the information below to determine the app's OWASP level. IF *Mobile* = Y IF "personal and/or sensitive data is accessed, processed, or stored" = Y OWASP level then MASVS = 2 IF sensitive data is persisted to the device then MASVS = 2+R ELSE OWASP level then MASVS = 1 IF *Web* = Y IF "personal and/or sensitive data is accessed, processed, or stored" = Y OWASP level then ASVS = 2 ELSE OWASP level then ASVS = 1	ORCHA
6b — Q8	Does the application connect to national/regional EHRs?	ORCHA
6b — Q9	Does the application provide alerts or notifications?	ORCHA

	Criteria	Criteria Origin
6b — Q10	Does the application provide suggestions?	ORCHA
6b — Q11	Does the application undertake calculations?	ORCHA
6b — Q12	Does the application support in-application purchases?	ORCHA
6b — Q13	Has a security assessment been undertaken by an accredited external third party?	ORCHA
6b — Q14	Is the external third party a CREST/APMG/CHECK registered supplier?	ORCHA
6b — Q15	Does the scope of the report cover the full technical architecture of the application?	ORCHA
6b — Q16	Has an industry standard been used for the risk model in the associated PEN/vulnerability testing?	ORCHA
6b — Q17	Have all *medium* risks/issues identified been mitigated and resolved, and can this be demonstrated through retesting within six weeks of the original PEN/vulnerability testing?	ORCHA
6b — Q18	Has the PEN testing been undertaken within the last 12 months?	ORCHA
6b — Q19	Has the code-level security assessment been undertaken against the correct OWASP level?	ORCHA
6b — Q20	Is the methodology for the security review proportional to the attack service and risk of the application?	ORCHA
6b — Q21	Does the organization have CyberSecure Canada certification?	MHCC
6b — Q22	Does the organization have CIS Top 20 Compliance?	US DHAF
6b — Q23	Does the organization have SOC-2 certification?	US DHAF
6b — Q24	Does the organization have ISO 27001 certification?	ORCHA

7. Cultural Safety, Social Responsibility, and Equity Standards

7a. Data

	Criteria	Criteria Origin
7a — Q1	Is the user made aware that there is an option to use an alias name instead of their own when signing up?	MHCC
7a — Q2	Is the privacy policy readable at a Grade-5 level or below?	MHCC

7b. Data and Indigenous people in Canada

	Criteria	Criteria Origin
7b — Q1	Is the product aimed at Indigenous users, or is it likely to be used by them?	MHCC
7b — Q2	If the data relates to an Indigenous population, has the user been informed about the level of their retained ownership of data that is shared with third parties?	MHCC
7b — Q3	If the data collected relates to the Indigenous people and communities, has the data selected for collection been reviewed or agreed to by the First Nations Information Governance Centre (FNIGC), or has it achieved OCAP (ownership, control, access, and possession) accreditation?	MHCC
7b — Q4	If this tool contains data relating to an Indigenous population, has the security of the data taken into account the OCAP principle of ownership?	MHCC
7b — Q5	If this tool contains data relating to an Indigenous population, has the security of the data taken into account the OCAP principle of control?	MHCC

	Criteria	Criteria Origin
7b — Q6	If this tool contains data relating to an Indigenous population, has the security of the data taken into account the OCAP principle of access?	MHCC
7b — Q7	If this tool contains data relating to an Indigenous population, has the security of the data taken into account the OCAP principle of possession?	MHCC
7b — Q8	Is the app *particularly likely* to be used by Indigenous users, even if they are not the primary market for the product?	MHCC
7b — Q9	Has a process been designed and put in place that allows Indigenous users to easily access, understand, and exercise their own data protection rights?	MHCC
7b — Q10	Have Indigenous users been consulted when designing this processing practice?	MHCC
7b — Q11	Does the policy specify that the developer will reobtain Indigenous users' consent (1) if the information collected materially changes, (2) the purpose for which the information is processed changes, or (3) the information is to be offered to new/different third parties?	MHCC
7b — Q12	Is there a separate policy (or section in the privacy policy) specifically designed to inform Indigenous users of their rights, in keeping with First Nations principles?	MHCC
7b — Q13	When marketing the product outside their country of residence, has the developer considered other jurisdictional laws and principles regarding Indigenous users?	MHCC
7b — Q14	Does the policy specify the types of personal data that will be collected from Indigenous users?	MHCC
7b — Q15	Does the policy specify how the developer will use the personal data collected from Indigenous users?	MHCC
7b — Q16	Does the policy specify whether such personal data will be shared with advertisers or other third parties?	MHCC

7c. Clinical evidence

	Criteria	Criteria Origin
7c — Q1	Please select whether there is supporting evidence for any specific populations.	MHCC
7c — Q2i	Where health-care professionals are involved, do they represent 2SLGBTQ+ communities?	MHCC
7c — Q2ii	Where health-care professionals are involved, do they represent Black, Indigenous, and people of colour (BIPOC) communities?	MHCC
7c — Q2iii	Where health—care professionals are involved, do they represent persons with disabilities?	MHCC
7c — Q3	If the app talks about religion and spirituality, is there evidence-informed data to support the effectiveness of religion and spirituality?	MHCC

7d. Clinical safety

	Criteria	Criteria Origin
7d — Q1	Do the hazard log and safety case mention BIPOC communities?	MHCC
7d — Q2	Do the safety case and hazard log ensure that any potential risks for BIPOC communities have been mitigated?	MHCC

7e. Usability and accessibility

	Criteria	Criteria Origin
7e — Q1i	Is the information on the app tailored to a specific culture/community?	MHCC
7e — Q1ii	Which culture/community is the app tailored to?	MHCC
7e — Q2i	Is the information on the app tailored to a specific province, territory, region, or geographic area?	MHCC

	Criteria	Criteria Origin
7e — Q2ii	If yes, which province(s), territory(ies), region(s), or geographic area(s) is the app tailored to?	MHCC
7e — Q3	Does the app include any visual representations or images of people?	MHCC
7e — Q4	Are visuals on the app representative of at least one 2SLGBTQ+ identity/community?	MHCC
7e — Q5	Is there 2SLGBTQ+ representation in information/examples?	MHCC
7e — Q6	Can users enter gender information into the application?	MHCC
7e — Q6i	Can the user opt out of sharing their gender identity?	MHCC
7e — Q6ii	Select which gender identities are available on the app.	MHCC
7e — Q6iii	Is there a free text space for people to self-describe?	MHCC
7e — Q7i	Is the language gender neutral? (no uses of he/him, she/her)	MHCC
7e — Q7ii	Is the language gendered because the user was able to input a preferred pronoun/gender?	MHCC
7e — Q7iii	Is the app written in Canadian French?	MHCC
7e — Q8	Is the app 2SLGBTQ+ inclusive?	MHCC
7e — Q9	If the app is tailored to 2SLGBTQ+ (If 7e — Q1i = Yes): Have the app developers received appropriate 2SLGBTQ+ awareness training and/or do they have lived and living experience?	MHCC
7e — Q10	Is the app available in non-official languages spoken in Canada?	MHCC
7e — Q11	Is the app available in any Indigenous languages?	MHCC
7e — Q12	Are there cultural and/or Indigenous resources on the app?	MHCC
7e – Q13	Are visuals on the app representative of BIPOC communities?	MHCC
7e — Q14	Is the app inclusive toward the BIPOC community?	MHCC

	Criteria	Criteria Origin
7e — Q15	Have the app developers received appropriate BIPOC awareness training and/or do they identify with this community?	MHCC
7e — Q16	Are visuals on the app inclusive toward persons with visible disabilities?	MHCC
7e — Q17	Is the text on the app readable at the Grade-5 level or below?	MHCC
7e — Q18i	Does the app have any audio?	MHCC
7e — Q18ii	Is audio supported with the use of captions?	MHCC
7e — Q19i	Does the app have any videos?	MHCC
7e — Q19ii	Is video supported with the use of sign language in the app?	MHCC
7e — Q20	Is the app accessible to persons with disabilities?	MHCC
7e — Q21	Have the app developers received awareness training for persons with disabilities and/or do they identify with this community?	MHCC
7e — Q22	Is the app presentation free from bias?	MHCC

8. Enhanced Data Sovereignty Standards

This domain of the framework adopts the CIHI (Canadian Institute for Health Information) minimum standard for collecting race-based and Indigenous identity data in health care. As that guidance document explains, while there are many benefits to collecting this variety of data, there are risks and barriers to assess and mitigate. To identify and address inequities in digital mental health care, prioritizing the safe and appropriate collection and use of this data will be essential (p. 5).[8] Appendixes A and B provide glossaries of the key concepts and relevant terminology used in this section.

[8] Canadian Institute for Health Information. (2022). *Guidance on the use of standards for race-based and Indigenous identity data collection and health reporting in Canada*. https://www.cihi.ca/en/race-based-and-indigenous-identity-data

8a. Engagement, governance, access, protection (EGAP) and ownership, control, access and possession (OCAP®)

	Criteria	Criteria Origin
8a — Q1	Has the company specifically tasked a representative with considerations on data sovereignty?	MHCC
8a — Q2	If not, does it consider data sovereignty when collecting ethnicity/race data?	MHCC

8b. EGAP

	Criteria	Criteria Origin
8b — Q1	Do you engage, listen, and act on the statements of ethnic minority communities and their members (including the most marginalized) regarding processing racial/ethnic data?	MHCC
8b — Q2	Can it show evidence of ongoing consultations with ethnic minorities throughout the development of the app? **Guidance:** Do they continue to listen (according to a schedule) after the initial planning stages?	MHCC
8b — Q3	Can the developer show evidence of techniques being used when collecting data (e.g., phone, face-to-face, group discussions)?	MHCC
8b — Q4	When collecting race-based data, do individuals give the company informed consent to use their data?	MHCC
8b — Q5	Can it show evidence of an explicit agreement not to share, sell, or otherwise use an individual's race-based data for a new purpose?	MHCC
8b — Q6	Does it carefully process individual data while being vigilant not to harm minority communities?	MHCC
8b — Q7	Does it take accessibility into account?	MHCC

	Criteria	Criteria Origin
	Guidance: Does the company consider various languages, formats, and individuals with disabilities when handling and sharing data?	
8b — Q8	Does it prioritize minority communities and their responses?	MHCC
8b — Q9	Has it set targets for addressing health inequities?	MHCC
8b — Q10	Does it have targets for progress monitoring?	MHCC
8b — Q11	Does the developer hold some accountability toward minority communities?	MHCC
8b — Q12	Can it show evidence of work being done to understand what communities look like in different areas?	MHCC
8b — Q13	Can individuals access their collective data and determine who else can access it (without any barriers)?	MHCC
8b — Q14	Is there evidence that capacity and infrastructure needs are being accounted for? **Guidance:** For example: facilitating training or teaching community members how to communicate using data, analyzing data, and connecting with required technology.	MHCC
8b — Q15	Does it allow external researchers or organizations access for the purpose of collecting new and current data?	MHCC
8b — Q16	Can it show evidence that all individuals' rights and data — including identifiable, de-identified, and anonymized data — are protected?	MHCC
8b — Q17i	Have data collectors explained why they are asking for race-based data?	MHCC
8b — Q17ii	Have data collectors explained what the race-based data will be used for?	MHCC
8b — Q18	Have data collectors explained how race-based data will be stored?	MHCC
8b — Q19	Have data collectors explained who will have access to race-based data?	MHCC

	Criteria	Criteria Origin
8b — Q20	Is the individual's right to informed consent and refusal protected from harm or damage with appropriate safety measures?	MHCC
8b — Q21	Has the developer clearly told individuals that providing data is not required to receive care and that refusal will not impact their quality of care?	MHCC
8b — Q22	Does the developer use additional protective measures when there is a high risk that an individual will be identified?	MHCC
8b — Q23	Can it show evidence of specific protection that focuses on preventing all data from being misused?	MHCC

8c. OCAP

	Criteria	Criteria Origin
8c — Q1	Does the company collect and store data the same way for every community (including minority ethnic groups) — that is, as it would for an individual whose rights or data use is protected?	MHCC
8c — Q2	Do you identify First Nations in your data?	MHCC
8c — Q3	How are First Nations identified in its data collection?	MHCC
8c — Q4	Does the developer provide details on who owns the data?	MHCC
8c — Q5	Does it make data available under licence, so that its ownership and terms of use are clear?	MHCC
8c — Q6	How does the company establish ownership?	MHCC
8c — Q7	Does it document how consent is managed? **Guidance:** That is, how individuals consent to data usage and storage, and giving them the right to withdraw their consent.	MHCC
8c — Q8	Are First Nations given control over their people, communities, and representative bodies?	MHCC
8c — Q9	Do First Nations have control over how data is collected, used, and disclosed?	MHCC

	Criteria	Criteria Origin
8c — Q10	Are there any agreements in place regarding control over data?	MHCC
8c — Q11	What is the company's decision-making process for the use of data?	MHCC
8c — Q12	Does it document data flow, outlining how it is transferred and used?	MHCC
8c — Q13	If yes, does the data flow documentation include what is done after it has been used for all intended purposes?	MHCC
8c — Q14	Does it provide First Nations with access to information and data about themselves and their communities, regardless of where they are held?	MHCC
8c — Q15	Does the company clearly state who has access to what data?	MHCC
8c — Q16	Is training/education provided to all those who have access to data?	MHCC
8c — Q17	What data access security/privacy policies and procedures are in place?	MHCC
8c — Q18	Does it clearly state that data will be held by a First Nation or a First Nation-controlled entity?	MHCC
8c — Q19	For any data not held by a First Nation or a First Nation-controlled entity, what is the explanation?	MHCC

Appendix A

Distinguishing race and ethnicity[9]

The terms "race" and "ethnicity" are often used interchangeably or as a single, conflated construct — "race/ethnicity." However, race and ethnicity are distinct social constructs, and the measurement and reporting of racial and ethnic health inequalities should reflect these differences.

Race is a social construct used to judge and categorize people based on perceived differences in physical appearance in ways that create and maintain power differentials within social hierarchies. There is no scientifically supported biological basis for discrete racial groups.

Racialization is the process by which people are judged and categorized into races primarily using differences in physical appearance. In this process, societies construct races as "real," different and unequal in ways that pertain to economic, political and social life.

Ethnicity is a multi-dimensional concept referring to community belonging and a shared cultural group membership. It is related to socio-demographic characteristics, including language, religion, geographic origin, nationality, cultural traditions, ancestry and migration history, among others.

A glossary of key concepts and relevant terminology is in Appendix B.

[9] As cited (p. 5) in Canadian Institute for Health Information. (2022). *Guidance on the use of standards for race-based and Indigenous identity data collection and health reporting in Canada*. https://www.cihi.ca/en/race-based-and-indigenous-identity-data

Appendix B

The glossary below presents a list of key terms and concepts used in [the Enhanced Data Sovereignty Standards domain], as well as their definitions. It is provided to clarify the language, avoid the conflation of concepts, and distinguish these terms and concepts from colloquial language and understandings, where applicable.

Glossary[10]

culture. The overt and subtle value systems, traditions and beliefs that influence our decisions and actions.

distinctions-based. An approach that aims to avoid conflating the Indigenous Peoples within Canada, and instead recognizes First Nations, Inuit and Métis as separate groups, each with their own diverse cultures, traditions, communities and histories. A distinctions-based approach ensures that the unique rights, interests and circumstances of each of these groups are acknowledged, affirmed and implemented.

health equity. The absence of unjust, avoidable differences in health care access, quality, experience or outcomes.

health inequality. Differences in health between individuals, groups or communities. Measuring health inequalities is a first step toward identifying and reducing health inequities.

Indigenous data sovereignty. The collective and individual rights of Indigenous Peoples to the self-governance and management of data from and about their communities, lands and individuals.

racialized group. A social construct describing groups that have racial meanings associated with them that affect their economic, political and social life. This term is sometimes preferred over "race" because it acknowledges the process of racialization.

racism. Includes thoughts or actions that establish or reinforce the superiority or dominance of one racialized group over another. Racism exists on a spectrum and acts on multiple levels — internalized, interpersonal and systemic.

internalized racism. The acceptance by a marginalized racialized group of negative messages concerning their abilities and worth.

---

[10] As cited (pp. 21-2) in Canadian Institute for Health Information. (2022). *Guidance on the use of standards for race-based and Indigenous identity data collection and health reporting in Canada*. https://www.cihi.ca/en/race-based-and-indigenous-identity-data

interpersonal racism. Racism that occurs when an individual experiences discriminatory behaviour from others.

systemic racism. Racism that occurs at societal and organizational levels, giving rise to the other forms of racism. It is often pervasive and subtle, and not always intentional. It is embedded in societal and institutional policies, regulations, legislation and ideologies that perpetuate racial disadvantage.

self-determination. A principle that concerns a person's or nation's right to determine and have control over their own future, political status, culture, economy and independence.

Mental Health Commission of Canada
Commission de la santé mentale du Canada

Mental Health Commission of Canada, 2021
Suite 1210, 350 Albert Street
Ottawa, ON. K1R 1A4
Tel: 613.683.3755
Fax: 613.798.2989

@MHCC_ /theMHCC
/1MHCC @theMHCC
/Mental Health Commission of Canada
/theMHCC