Canadian National Roundtable Discussions to Advance Regulation of Digital Mental Health

August 2021

Prepared by

Yuri Quintana, Ph.D.,
Chief, Division of Clinical Informatics, Beth Israel Deaconess Medical Center,
Collaborating Scientist at Homewood Research Institute,
Assistant Professor, Harvard Medical School

Farooq Naeem, MD,
The Centre for Addiction and Mental Health

Mary Jane Dykeman, JD
Managing partner at INQ Law

Waël Hassan, Ph.D.,
CEO, KI Design

Nelson Shen, Ph.D.
CIHR Health System Impact Fellow,
Centre for Addiction and Mental Health

Prepared for Homewood Research Institute

Funded by the McConnell Foundation

Funding for this report has been generously provided by:

The McConnell Foundation

Homewood Research Institute (HRI) is a registered Canadian Charity dedicated to transforming mental health and addiction treatment through research. We partner with leading scientists, universities, patients, and clinicians to improve care, services, and outcomes. HRI's charitable registration is # 86307 3334 RR0001.

Suggested Citation: Quintana, Y, Naeem F, Dykeman, MJ, Hassan W, Shen N. Homewood Research Institute Report, Guelph, Ontario, Canada, August 13, 2021. Available free of charge at URL: https://hriresearch.com.

This information can be made available in alternative formats upon request. Please contact us for assistance (info@hriresearch.com or 519-838-8104, ext. 32160)

Note: The opinions and recommendations included in this report are those of the authors and do not necessarily reflect the views of the funder.

Please Consider Making A Donation.
With your support, HRI can continue to conduct research and evaluation to pursue our vision of a world where.... *No life is held back or cut short by mental illness and addiction https://hriresearch.com/donate/donate-now/*

Executive Summary

Access to mental health and addiction treatment services is a challenge worldwide. The use of digital tools has great potential to address service access challenges. Digital tools and services claiming to promote mental health and wellbeing are proliferating rapidly. But these digital tools and services are coming onto the market in an unregulated environment, with no reliable information about efficacy, safety, or issues related to privacy and data security. Thus, it is difficult for potential users, especially clinicians, healthcare organizations, health systems, and community agencies, to adopt and use such tools with confidence.

Recognizing the potential value of regulation in this field, the McConnell Foundation funded this project through Homewood Research Institute. It was led by Yuri Quintana, Ph.D., Chief, Division of Clinical Informatics, Beth Israel Deaconess Medical Center and Collaborating Scientist at Homewood Research Institute, who served as Chair, supported by four Co-Chairs: Farooq Naeem, MD, The Centre for Addiction and Mental Health; Mary Jane Dykeman, J.D., Managing partner at INQ Law; Waël Hassan, Ph.D., CEO, KI Design; and Nelson Shen, Ph.D. CIHR Health System Impact Fellow, The Centre for Addiction and Mental Health.

Two Canadian National Roundtable meetings were held virtually on May 25 and 26, 2021, to discuss how to improve digital mental health services and apps, including their efficacy, safety, security, and privacy. A total of 90 invited participants engaged in the Roundtables; they included healthcare professionals, representatives from government, not-for-profits, and companies in digital mental health and people with lived and living experience and advocates for mental health in Canada. The Chair and Co-Chairs distilled the discussions and drafted recommendations reviewed at a third virtual Roundtable held June 16, 2021. The group identified areas that need policy improvements and articulated strategies to improve the engagement of stakeholders with the end goal of implementable solutions. Discussion points are summarized in this document. The main themes and recommendations are as follows:

1. **What:** A system for review of digital mental health apps be established to include efficacy, safety, privacy, and security that is transparent and evidence-based.

2. **How:** While a legislative response from any level of government in Canada may be difficult to achieve in the short term, an assurance program (not a certification nor compliance program) could be established, similar to Ontario Health's virtual visits verification platform for virtual platforms delivering healthcare, that can lead to a more formal accreditation process.

3. **Who:** A community of practice drives input from key stakeholders (public, industry, governments, regulators, healthcare associations, insurers), and that an assurance framework could be developed as a starting point toward regulation of digital apps and digital mental health apps more specifically.

4. **What else:** More resources and programs for the public and healthcare providers are required to guide the efficacy, safety, privacy, and security considerations of digital mental health apps.

Background

Access to mental health and addiction services is a challenge worldwide. These challenges have grown with both increased service demand and need for isolation during the pandemic. Mobile apps and other digital therapies could potentially respond to the growing need for services that complement face-to-face treatment.

However, it is vital to ensure that these digital therapies are effective and include appropriate safeguards. Given the rapid proliferation of digital services, accelerated by COVID-19, there is an urgency to identify how we can rigorously evaluate digital mental health tools and what policy improvements are needed to address efficacy, safety, privacy, and security concerns.

Mobile apps are being developed and deployed in record time in a highly unregulated environment. On the one hand, this is exciting because it exponentially expands the pool of tools available. On the other hand, important concerns arise. For instance, it is often unclear which apps are solely intended for wellness or therapeutic use. Especially for tools intended for therapeutic use, there is a need to assess efficacy, safety, and privacy. This is particularly important for tools intended to be used by healthcare providers or within healthcare systems.

It is unclear who should be tasked with evaluating claims of efficacy by app vendors, given that apps are globally available through various platforms. However, rigorous and transparent evaluations are needed to ensure that consumers and multiple healthcare systems can use these digital tools with confidence as they deliver mental health and addiction services.

Digital apps can collect vast amounts of personal data, including personal health information. Users may be unaware of subsequent uses and disclosures that may be made. The implications for privacy and information security are concerning, especially given the risks of cyber breaches and uneven accessibility of privacy policies and terms of use.

Additional regulatory oversight and policy improvements may be required to promote informed decision-making and address concerns of healthcare providers and community service organizations considering incorporating mobile apps into their clinical practices.

Roundtable Process: Discussion Topics and Major Points Raised

a) Evaluating the Efficacy of Digital Mental Health Tools

At the first Roundtable, stakeholders considered how to evaluate and regulate the efficacy of health and wellness apps in this relatively new digital mental health environment.

COVID-19 accelerated the already rapid development of apps and virtual platforms across the health system. Unfortunately, there is no single clearinghouse to determine the purpose of a given app (therapeutic vs. wellness uses), nor are apps subject to review for claims they make or imply regarding their efficacy.

There is more than one way to regulate the review of efficacy. One response could be legislative, but the goal of the Roundtable was to ensure that any recommendations are highly practical and 'implementable.'

Most agreed that a legislative response might not be the optimal approach at this time, given the length of time it typically takes to implement legislation. It was also noted that it is challenging to keep legislation and review processes current as technology changes and existing apps are further iterated, and new ones come to market. Any legislative response would also have to consider which level of government (federal, provincial/territorial) would be best placed to lead this, and there would have to be a willingness to take legislative responsibility for this issue. App developers would likely want a say in this, given that as they expand services in a growing market, they would have to navigate multiple jurisdictions' laws.

A new (or more likely, existing) body could also be tasked to issue guidance to the industry or set standards. It is unclear if health regulatory bodies (i.e., Health Colleges) would want to fill the gap to create rules to establish efficacy. University research groups or the private sector could be important stakeholders and those tasked with consumer protection and associations representing healthcare providers (including mental health).

The participants wondered if a consumer-driven review might be the most straightforward route, with an app rated by those who use it. But there were concerns about this: participants discussed expectations of patients and healthcare providers that therapeutic tools would be evaluated in line with scientific standards and values to ensure scientific rigour, management of conflicts of interest, and independent evaluation. Finally, the group wondered whether a group like Ontario MD, which has taken an active role in supporting the Canadian Medical Protective Association and Healthcare Insurance Reciprocal of Canada, might guide their members contemplating incorporating apps into clinical practice.

The group discussed the challenges of implementing a review process for digital mental health apps. Practical considerations such as the appropriate timeframes for review were raised. Some consumer-facing apps may be implying therapeutic benefits through marketing. There was discussion about instituting a warning label that could signal consumers that they are downloading or purchasing an app that may not have been evaluated for clinical efficacy (vs. finding this disclaimer only in the fine print of terms of use).

There also were questions about whether guidance documents for industry, healthcare providers, and the public are adequate and appropriate. If a consumer has a complaint, there is a question of where to take the complaint - whether to the company, a regulator, consumer protection organization such as Better Business Bureaus or equivalent bodies or to government, to name just a few.

b) Policies and Regulations for Privacy and Security in Digital Mental Health

On Day 2 of the Roundtable, participants explored the privacy and security implications of the widespread use of digital mental health apps.

The panel noted that it is unclear how aware a typical app user is of the amount and type of data apps may collect, for what purposes, and how information may be used and disclosed.

Although federal legislation, *Personal Information Protection and Electronic Documents Act (PIPEDA),* would apply to app developers, and applicable provincial and territorial legislation (including Ontario's *Personal Health Information Protection Act (PHIPA), 2004*) would apply to healthcare providers who integrate apps into the treatments and services they provide to patients, it is unclear what a typical app user knows about this legislation.

COVID-19 was once again cited as a driver for the adoption of virtual care, mobile apps, and other technology. This had been noted early in the pandemic by the federal Privacy Commissioner, Daniel Therrien, in a statement to govern the significant demands on personal information and technical tools that emerged: A Framework for the Government of Canada to Assess Privacy-Impactful Initiatives in Response to COVID-19 - Office of the Privacy Commissioner of Canada

The Roundtable heard briefly about PHIPA's contemplated oversight of "consumer electronic service providers." It was acknowledged that if enacted, the detail will be in regulation. At least for now, the intent is to enhance disclosure of a patient's personal health information at their request, to their chosen vendor, as a potential alternative to PHIPA's rules for individuals wishing to access their personal health information. At this time, it is unclear how these rules for consumer electronic service providers might be related to themes and recommendations of this Roundtable report.

Another significant factor is the federal government's introduction in late 2020 of Bill C-11. If passed, the *Digital Charter Implementation Act* and the *Consumer Privacy Protection Act (CPPA)* would modernize PIPEDA. The CPPA would take Canada one step closer to Europe's General Data Protection Regulation (GDPR) and create many new rules that could benefit consumers wishing to control their data better while placing requirements on the private sector, including app developers.

Short of amendments to privacy or consumer protection legislation, a consideration is whether governments should or would consider the adoption of specific standards to govern consumer apps. An example exists in Ontario; it involves Ontario Health, in conjunction with OntarioMD and the Ontario Telemedicine Network. This assurance process established a verification protocol to assess whether the technology provider meets specific standards, such as having a privacy impact assessment completed by someone with specifically established credentials or with a certain number of years of experience in privacy. In this way, there is at least some measure of assurance in place. However, it is neither certification nor a full compliance assessment: Verified Solutions | Virtual Visit Solutions for Healthcare Providers. This is an example of a government not legislating requirements but establishing standards for technology providers to meet as part of an assurance program.

c) Privacy Notices and Informed Consent

There is a challenge in the health sector with privacy policies and terms of use that healthcare organizations and private companies make available to consumers. Many statements are very long and complex; the process does not lend itself well to grounding notice, much less informed consent. The app user may choose not to read these documents, but the focus must be on ensuring that users are made aware if they wish to be, that their information is at play. Whose role is it to set this standard? The federal Privacy Commissioner or provincial/territorial counterparts have noted fundamental issues with opaque privacy policies and terms of use in the past.

In short, app users must know what information they are providing and why, who will have access to it for what initial purpose, and whether there are any secondary uses or disclosures that could or will be made later. It must be clear what happens if they withhold or withdraw their consent to provide this information to the app developer, whether this limits their ability to use the app, in whole or in part. The requirements for breach notification already apply to companies and organizations in Canada. However, it is essential that the developers who create mobile apps and healthcare providers who use them in clinical practice also know how to mitigate any breaches and report them as the law requires. In the event of a breach, the regulator may issue a decision or order to address the source of the breach.

The idea of “informed” in informed consent was questioned by Roundtable participants because there is an unreasonable level of literacy required to comprehend a typical privacy policy and terms of use terms of service. This is at odds with the ideals of knowledgeable and informed choice. It was noted that literacy might vary by population, exacerbating the effects of the digital divide and digital health equity. At the federal level, there has been guided by the Office of the Privacy Commissioner of Canada (OPC) in the form of best practices for communicating privacy policies for mobile apps (Mobile apps - Office of the Privacy Commissioner of Canada). There is also guidance for the broader private sector through recommendations on modernizing consent by avoiding information overload and facilitating understanding by emphasizing certain elements and allowing control of the level of detail (Guidelines for obtaining meaningful consent - Office of the Privacy Commissioner of Canada).

To start the discussion, the Roundtable was presented with a list of existing recommendations by the OPC on meaningful consent guidelines and Canada Health Infoway’s Pan-Canadian stakeholder workshops on consent. The recommendations include: what is collected; whom it is shared with; for what purpose; what are the risks; what are the service providers’ responsibilities; who has oversight; and how to revoke consent.

The core of the discussion was transparency, asking how we can bridge the literacy gaps and build trust. It was recognized that there needs to be more innovation in privacy notices, extending beyond “plain text.” Integration of visual aid and multimedia was seen as a potential approach to improve reader understanding. Some participants discussed the prospect of using machine learning and artificial intelligence to support decision-making. Consideration of accessibility and user experience and the user interface is required, especially with smartphone applications, where there are small screens.

High value was placed on human-centered design and participatory processes where diverse end-users are meaningfully engaged from the start. This process shape notices to respond to user preferences, needs, and experiences rather than designing notices based on traditional assumptions. This may enable a greater understanding of pain points and opportunities for microlearning on the concept of risk. Lessons or guidance on effective engagement and co-design can be gleaned from examples identified by the Roundtable (e.g., Foundry, Sage Bionetworks, FRAYME).

Some agreed there is a need for a dynamic approach to notices, recognizing needs of individuals change. As consent fatigue and consent apathy are challenges in the practice of digital health consent, individuals need the ability to control the level of detail they require, desire, or need at the moment.

For example, the privacy notice approach was taken by Health Canada's COVID Alert digital contact tracing app COVID Alert: COVID-19 Exposure Notification Application Privacy Assessment provides users with high-level details and allows them to drill down to the level of detail desired, including the threat risk assessment summary. Other notable cases exist with the major digital technology providers. For instance, Apple has leveraged privacy and trust as a commercial opportunity by focusing on timing and control, providing users with options for customized installation and just-in-time notifications. While the consent options are not comprehensive, the dynamic options provide users with a good consent experience and control.

The ability to control and allow users to see who is collecting, using, and disclosing data is critical in addressing privacy concerns related to mental health data and building trust. There was an identified need for developers to map the proposed data flow in their notices to support greater transparency. However, it was recognized that the data flows are often complex and challenging for users to grasp and to frame in the context of citizen rights and ethical use.

The Canadian Research Insights Council (CRIC) Canadian Code of Market, Opinion, and Social Research and Data Analytics was suggested as a source that may guide ethical use. Moreover, it was recommended that Privacy by Design certification may be a heuristic to signal that protective, preventative efforts to protect user privacy must always be the default and built into the design and architecture of the service (i.e., minimal information collected).

Legislative adherence by vendors is also an issue. From the patient/consumer perspective, how can applicable legislation be made more accessible and transparent? Given the multitude of permutations of vendor types (commercial, public), data hosting locations (domestic, international), and legislative jurisdictions (provincial/regional, federal, international), the layers of complexity are challenging for vendors to navigate, and demonstrate full compliance.

Questions were posed about how we foster transparency and trust in a siloed "individualistic" ecosystem and how it could benefit from more transparency that might be achieved through collaborative innovation, thereby sharing innovative practices and collectively demonstrating and reporting compliance.

Clarity is also required on the role of healthcare institutions in this dynamic as a potential intermediary between service providers and patients; and from a legal/liability perspective, what is the exposure for healthcare organizations, healthcare providers, or community service organizations that use such apps in their clinical practice and recommend them to patients?

d) What are current concerns and gaps in data security and compliance for digital mental health?

With respect to data security, considerable emphasis was placed on what standards should exist, given consumers' apparent willingness to provide their personal information, including personal health information, via an app, in return for a benefit. In this context, what is the standard to be applied, and who will have oversight? Or should there be guidance that enables an app developer to be seen as a good corporate citizen by submitting a review for the app?

Again, a challenge is federal versus provincial laws on privacy (and therefore on security) and the division of powers between federal and provincial governments over healthcare regulation. Typically, an organization takes steps, sometimes recommended by their legal counsel or insurers, or their IT departments, to implement a robust information security policy. On the other hand, the average consumer may be unaware of the inherent risks of unsecured devices or devices that track them using their phones. They may unknowingly continue to provide sensitive information about their health, family matters, and more. In many workplaces, there are corporate policies regarding device security. However, not every consumer reads an app's terms of use and privacy policy closely, and some of these documents lack transparency.

There was also a discussion about where data is hosted. There has been debate over many years in Canada around personal information stored in the United States. In most provinces, this is not prohibited. An emerging issue identified is cloud-based services, i.e., do they help or hinder privacy and security compliance or the responsible use of data.

Key Discussion Points

a) The need for frameworks or standards

Nearly all participants emphasized the need for a framework to govern apps, or at minimum (if not enshrined via legislation), strong standards or directives clearly articulated for app developers. We heard that developers were not opposed to complying with standards, as long as they are clear and practical. Some noted that medical devices are highly regulated, in contrast to software serving as a medical device and apps more generally. Some said that if there were a straightforward way to comply with applicable rules and receive a stamp of approval, app developers and IT professionals would do it because it is good business to do so.

Participants generally agreed that a broad range of stakeholders should be engaged in establishing this process for oversight. It is essential to consider all relevant evaluation perspectives: academic, app developer, intended end-user, and regulatory experts.

Similarly, a need was emphasized to disseminate knowledge and standards in critical areas. There was some focus on how to do this well without creating an undue burden yet benefiting consumers. Participants liked the notion of clear and transparent rules: clear expectations for developers and transparent and accessible labelling for users. The challenge of digital literacy among the public was acknowledged; one participant noted a need for public education on labelling so that Canadians know what to look for when purchasing/using an app in this space.

b) Guided Self-Regulation by Developers

An issue highlighted was terminology and how app developers may characterize their apps as they see fit. For example, they may say they have a wellness app, which does not attract the same scrutiny as a therapeutic mental health app. Again, the participants stressed the importance of educating the public, given the proliferation of apps available and in the pipeline. Consumer awareness is vital to a model of standard-setting for mobile apps and other virtual platforms. Participants stated that both the app users (consumers) and the healthcare providers who choose to use them in their clinical practice need varying degrees of information on their risks and benefits and a better understanding of the impact of making this choice.

To that end, concerns were raised about a clinician recommending a specific app, either in its own right or as part of a treatment or care plan. What accountabilities and liabilities arise? Will clinicians embrace apps, and will their insurers cover them for any novel claims about a patient's reliance on the app? These issues merit further attention. It is crucial that clinicians understand the app, particularly if they integrate such apps into their practices.

A few participants expressed concerns over governments and governmental agencies' lack of interest in app regulation. One participant suggested that some governments have been reluctant to engage in the issue given its complexity and a perception that engaging would not lead to a "win." Another participant said that it is improbable that the app regulations will come from the government, given that it remains a "messy" area of law and healthcare.

When discussing the qualities of an assessment and evaluation tool, participants reiterated multiple times that they would like any such tool to be practical and implementable. It cannot be a make-work project. Developers are willing to be part of the discussion and have rules imposed as long as they are clear and practical.

The need to adopt a scientific approach was also discussed. This is particularly important for digital tools in healthcare settings where they serve as medical devices.

One participant suggested a consensus/Delphi process to discuss framework development, then work with health organizations to study the implementation process.

The cost was said to be an essential consideration in designing an app evaluation process.

One participant suggested the effort needed focus and that the focus should be on apps intended to be used professionally within the healthcare system. Healthcare providers (both individual practitioners and healthcare organizations) need to recommend an app or digital intervention with confidence.

Notably, the US Food and Drug Administration has oversight for medical devices. It has proposed precise details for reporting requirements of efficacy and software requirements, but some participants viewed it as an overly cumbersome process. It was also stated that it is sometimes difficult to distinguish between software, firmware, and hardware. One participant noted that in the U.S., there might be a move toward considering apps as hardware. Those working in public and private sectors were unequivocal that there must be a transparent and implementable rule for digital mental health apps.

Other areas identified for further investigation include the need to study the consumer's journey to purchasing a given app and identify the decision points effectively and opportunities to inform and support sound decision-making. As noted above, there is also a need to measure and understand variations in customers' digital literacy skills.

Finally, participants agreed that the purpose of mental health apps is not to replace healthcare providers. People use mental health apps because they find what works independently to cope with whatever they face. The grey zone is the space between a wellness app versus a therapeutic app that a healthcare provider could endorse and rely on.

How does a consumer know that a given vendor is compliant with applicable laws and following best practices?

Three significant challenges for the digital mental health space were identified:

1. Many apps are not made in Canada but rather in the United States. This creates compliance challenges from security and privacy perspectives. In the U.S., and in Canada too, commercial enterprises are often not considered "covered entities" (a term found in U.S. health privacy legislation, the *Health Information Portability and Accountability Act* (HIPAA)); by contrast, healthcare providers in Canada are data stewards, health information custodians, trustees or equivalent. In the U.S., a company that is not a covered entity under HIPAA may have the freedom to use the data they hold without restrictions. As well, covered entities in the U.S. can de-identify data (remove 18 fields from a data set) and then do what they want with the data. Similarly, some labs and clinics are masking or de-identifying data in Canada and treating the resulting dataset as their property. For U.S. companies providing services in Canada, HIPAA does not apply. Consequently, decisions about collected data are left up to the company. There are many more U.S. companies than Canadian companies operating in the Canadian e-health space.

2. Many corporations rely significantly on their legal departments to produce compliance instruments (such as privacy policies and terms of use) and are well defended by these instruments. They appear to be compliant. However, in reality, their internal tools, systems, and processes may not live up to the outward-facing promises of their public statements.

3. There is currently a gap in the legal framework regarding community health, personal support, and e-mental health, including for organizations supporting youth in crisis or helping people with disabilities in various life challenges. This legal void creates an environment where compliance requirements are not defined, and therefore privacy and security implementation varies drastically from one healthcare provider to the next.

Compliance technologies were also discussed:

1. Audit. In Ontario, several hospitals have implemented predictive analytics and AI to detect unauthorized data access. Similar tools can be implemented for app service providers.

2. Zero-trust database systems. These systems are ones where even the administrator does not have access to the raw data. Using big privacy solutions, data elements are tagged so that each time data is used, that use is challenged and logged. With some privacy tools, only analytics are shared rather than identifiable data elements.

3. The use of technologies, including apps, that provide compliance checks, reminders, tracking of data within the enterprise, inventory of data released to partners, data erasure on demand, and providing individuals with copies of their data on demand.

From a design perspective, five aspects are currently missing from compliance – data collection, retention, protection, disclosure, and use for a purpose. It is essential to validate what is happening to data.

c) Dissemination Strategy

Similarly, a need to disseminate knowledge and standards in this area was emphasized. Participants liked the notion of clear, transparent, and available regulations for developers and clear labelling for end users. As there was a concern regarding digital literacy rates among the general public, a participant said that there is a need for public education (perhaps generally first and eventually, labelling of apps) so that Canadians know what to look for when purchasing/using an app. There was also agreement that public engagement with diverse perspectives is critical in co-designing accessible solutions to bridge the literacy and equity gaps.

d) Governance

When asked who should regulate apps, whether the federal government or provincial governments, not-for-profit groups, academic groups, private sector entities, regulators, associations or health regulatory bodies (such as health Colleges), or the Private sector- there were no clear answers, however, there was a consensus that a broad range of stakeholders should be engaged in this process. It is essential to have representatives from all perspectives of the evaluation: academics, app developers, intended end-users, and regulatory experts. It was further emphasized that without intervention from Apple or Google, we could not control those storefronts, and there is no nuance as to whether an app is for wellness (which may alleviate specific oversight) versus being employed for therapeutic purposes. Again, the participants stressed the importance of educating the general public. For the moment, we may establish ground rules for how informed the public is on apps; and help healthcare providers access helpful information. On the latter point, concerns were raised over healthcare providers prescribing apps to their patients. For example, suppose a healthcare provider recommends an app to be used as part of a treatment plan. In that case, is it possible that any harm arising from the use of the app by that patient could be attributed to the healthcare provider, even despite disclaimers of using the app at the user's own risk? Whether individual clinicians or organizations where they work, healthcare providers would do their due diligence on the risks and benefits of formally recommending apps. We can speculate that a patient whom a clinician tells to use a particular app will believe that it is safe to use. If they are harmed as a result (or even allege they were), that healthcare provider may need to answer questions regarding their due diligence in making the recommendation.

We recommend a governance model that identifies which agencies are responsible for the assurance, certification, and compliance assessment for clinical efficacy, safety, privacy, and security.

e) Evaluation Standards and Process

When discussing the qualities of an assessment and evaluation tool, participants said it must be practical and implementable. Participants noted that app developers need clarity around expectations placed on them about efficacy, safety, privacy, and security. The need to adopt a scientific approach was also emphasized. One participant suggested that there should be some consensus/Delphi process to discuss framework development and then work with healthcare organizations to study the implementation process. Cost considerations were also identified as a critical aspect of the app evaluation process. One participant wanted the framework to be feasible, focused, and practical; this individual further explained the term "focused" in this context. It would be helpful to focus on apps that are intended to be used professionally within the healthcare system; clinicians and healthcare organizations need to know how they can live with confidence how to recommend an app or digital intervention to a patient. In addition to affordability and cost, participants also considered outcomes and accessibility (access to technology) to be essential considerations in this regard.

Participants expressed the need for further clarifying concepts in this area, such as "what is good research, and what are the appropriate validity measures applicable to mobile apps in the context of mental health?" One participant offered that it would be interesting to collaborate with the ten most popular apps, integrate and coordinate the efforts. Obstacles in conducting high-quality research were also considered. Further research areas were identified, such as a need to study the consumer's journey to identify the decision points effectively and opportunities to inform and support sound decision-making. Need to understand variations in customers' digital literacy skills were highlighted. As one participant said, young people are competent today and know what a good app is and is not!

Conclusions

This report has summarized a discussion of many critical issues that need to be addressed to ensure the safety, efficacy, privacy, and security of digital mental health apps and related services.

The Roundtable sessions included a broad range of organizations and professional disciplines and had people with lived and living experience in mental health and substance use. It is clear from the breadth and depth of the discussions that these are complex issues that will require comprehensive stakeholder engagement to achieve solutions that meet the needs of a complex system of stakeholders.

There was a clear consensus in these Roundtables that there is a need for clear, transparent, and implementable processes for assurance co-developed with a broad range of stakeholders, including youth and people with lived and living experience. These processes will need to be evidence-based to evaluate the efficacy of mental health digital apps, with practical but reliable approaches for assessing privacy and security that can be updated as quickly as apps and technology change.

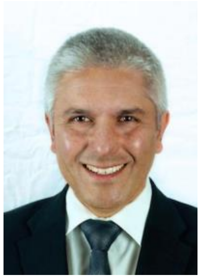
Finally, the need to have a dissemination strategy is needed for healthcare providers, citizens, and policymakers to educate all stakeholders on the issues and engage in developing solutions.

Key Themes and Recommendations

The themes and recommendations of this Roundtable are:

1. What: A system for review of digital mental health apps be established to include efficacy, safety, privacy, and security that is transparent and evidence-based.
2. How: While a legislative response from any level of government in Canada may be difficult to achieve in the short term, an assurance program (not a certification nor compliance program) could be established, similar to Ontario Health's virtual visits verification platform for virtual platforms delivering healthcare, that can lead to a more formal accreditation process.
3. Who: A community of practice drives input from key stakeholders (public, industry, governments, regulators, healthcare associations, insurers), and that an assurance framework could be developed as a starting point toward regulation of digital apps generally and digital mental health apps more specifically.
4. What else: More resources and programs for the public and healthcare providers are required to guide the efficacy, safety, privacy, and security considerations of digital mental health apps.

Biographies of Session Chairs



Yuri Quintana, Ph.D.
Chief, Division of Clinical Informatics, Beth Israel Deaconess Medical Center, Boston, MA, USA
Assistant Professor of Medicine, Harvard Medical School, Boston, MA, USA
Collaborating Scientist, Homewood Research Institute, Guelph, Canada,
Associate Professor, Health Information Science, University of Victoria, Victoria, BC, Canada

Yuri Quintana, Ph.D., is Chief of the Division of Clinical Informatics, Beth Israel Deaconess Medical Center, and Assistant Professor of Medicine at the Harvard Medical School. His research is focused on developing innovative technologies and systems that empower communities of healthcare professionals, patients, and families to collaborate on a worldwide basis. He has developed several global online collaboration networks for healthcare delivery and innovative applications in mobile health. Previously, Quintana was a principal investigator in the Canadian HealNet Research Network, focusing on consumer health informatics, and a faculty member at the University of Western Ontario. Quintana also served as director of the New Media Research Lab, developing interactive media and online education innovations. He has held high-tech positions at IBM Canada Limited and Watcom. He has been the Chair of five international conferences on medical informatics. Quintana obtained his engineering degrees from the University of Waterloo in Electrical and Computer Engineering and Systems Design Engineering.
Twitter: https://www.twitter.com/yuriquintana
LinkedIn: https://www.linkedin.com/in/yuriquintana/

Farooq Naeem, MD
The Centre for Addiction and Mental Health, Toronto, Ontario, Canada
Professor of Psychiatry at the University of Toronto, Toronto, Ontario, Canada

Dr. Farooq Naeem is a Professor of Psychiatry at the University of Toronto and a psychiatrist at the Centre for addiction and mental health. He was trained in Psychiatry in Merseyside training scheme in Liverpool, England. He completed his MSc in Research Methods in Health and Ph.D. at the Southampton University in England. He has pioneered techniques for adapting CBT across disorders and cultures. These techniques have been used to adapt CBT for various common and

severe mental health problems in South Asia, North Africa, the Middle East, and China. He has a keen interest in health systems. He has written six books and numerous book chapters. He has published nearly 200 papers in peer-reviewed journals. His research interests CBT, psychosis, and culture, with an overall aim to improve access to CBT. He works with a team of IT experts and has developed a CBT-based therapy program – called eGuru – that can be delivered through web and smartphone apps.
Twitter: https://twitter.com/farooqnaeem7
LinkedIn: https://www.linkedin.com/in/farooq-naeem-60a19a17/

Mary Jane Dykeman, JD
Managing partner at INQ Law, Toronto, Ontario, Canada

Mary Jane Dykeman is a managing partner at INQ Law. In addition to data law, she is a long-standing health lawyer, including in mental health. Her data practice focuses on privacy, artificial intelligence (AI), cyber preparedness and response, data governance, and digital health. She regularly advises on the use and disclosure of identifiable and de-identified data. Mary Jane applies a strategic, risk, and innovation lens to data and emerging technologies. She helps clients identify the data they hold, understand how to use it within the law, and how to innovate responsibly. Mary Jane has acted as in-house counsel to two Toronto teaching hospitals and the Psychiatric Patient Advocate Officer and was instrumental in the development of Ontario's health privacy legislation. She regularly consults on large data initiatives and the use of data for health research and quality purposes. Her consulting work extends to modernizing privacy legislation and digital societies and works with Boards, CEOs, and CIOs on the emerging risks and trends in data. Since 2004, she has taught Mental Health Law in Osgoode's Health Law LL.M. program (most recently with CAMH's Michele Warner). She is Deputy Chair of the Canadian Blood Services Research Ethics Board, chairs the Board of the Alzheimer Society of Toronto, and has recently been appointed to the advisory committee of the University of Toronto Temerty Centre for Artificial Intelligence and Education in Medicine (T-CAIREM).
Twitter: https://twitter.com/mjdykeman
LinkedIn: https://www.linkedin.com/in/mary-jane-dykeman-80ab1b22/

Waël Hassan, Ph.D.
CEO, KI Design, Toronto and Boston, MA, USA

Waël Hassan Ph.D. is one of North America's leading advisors in privacy

compliance, data management, and data analysis. He is the founder of KI Design, a US company that Designs and develops Big Data Analytics solutions. Clients include Nuclear Power Generation, Innovation Hubs, International Aide Organizations, Hospitals, Transportation and Aviation, Fortune 500, & Federal Government organizations. As CEO of KI Design, he has collaborated with a wide range of government and private-sector clients across different industries. He has in-depth knowledge of privacy laws across Canada and the US and holds the first Canadian Ph.D. in the validation of legal compliance. Waël is the author of "Privacy in Design: A Practical Guide to Corporate Compliance", "Using Social Media to Transform Election Monitoring", and "Implementing Data De-identification." All three books are hands-on and practice-based privacy resources. Waël maintains an active blog, waelhassan.com, providing thought leadership on AI, Big Data, Privacy & Security, Portfolio Management, and Governance. Moderates a "Media Analytics Club" at @clubhouse.
Twitter: https://twitter.com/drwhassan
LinkedIn: https://www.linkedin.com/in/drwaelhassan

Nelson Shen, MHA Ph.D.
CIHR Health System Impact Fellow, Centre for Addiction and Mental Health, Toronto, ON

Nelson Shen, Ph.D., is a Canada Health Institute of Research Health System Impact post-doctoral fellow embedded at the Centre for Addiction and Mental Health (CAMH). Nelson is also a course instructor in the Master of Health Information program at the Institute of Health Policy, Management, and Evaluation (IHPME), University of Toronto. His research focuses on patient engagement in designing and implementing digital health processes, policies, and innovations. His research interests include patient privacy, consumer health, behavioural theory, and design thinking. Nelson's dissertation focused on understanding patient privacy perspectives in the digital health environment. He was a privacy specialist at eHealth Ontario, focusing on projects related to consumer applications. His current privacy work includes collaborating with Canada Health Infoway to understand user and business requirements of implementing meaningful consent in digital health. Other works with Infoway focus on exploring adolescent consent to support adolescent access to their records.
Twitter: https://twitter.com/nelshen
LinkedIn: www.linkedin.com/in/nelshen

About Homewood Research Institute (HRI)

Homewood Research Institute (HRI) is an independent national charity dedicated to research that will transform mental health and addiction services across Canada and worldwide. We partner with leading treatment providers, universities, and research institutes, coordinating efforts to advance a common goal: improving treatment to save lives. Through HRI's strategic partnership with our founder and primary partner, Homewood Health, we are uniquely able to research a range of treatment settings across the country. This means that we work directly with our most significant stakeholders – people living with mental illness and addiction. We've also built vital academic partnerships with McMaster University, St. Joseph's Healthcare Hamilton, and the Peter Boris Centre for Addictions. We work with leading researchers at Western University, the Centre for Addiction and Mental Health, and Harvard. Our growing network includes some of the world's most influential scientists, clinicians, and researchers. Today, we are recognized as a national research institute, unique in our commitment to collaboration - rather than competition – to enhance treatment and lives. The work we do will advance services and improve the well-being of individuals, families, workplaces, and society.

The McConnell Foundation

The McConnell Foundation is a private Canadian foundation that develops and applies innovative approaches to social, cultural, economic, and environmental challenges. We do so through financial support and investing, capacity building, convening, and co-creation with grantees, partners, and the public. The McConnell Foundation has a vision for a Canada in which the economy and social systems advance the well-being of all people and in which the natural environment is stewarded for future generations. We are committed to reconciliation between Indigenous and non-Indigenous peoples and seek to unleash the resources and creativity of individuals and organizations from all sectors to solve social challenges.

https://mcconnellfoundation.ca/about-2/purpose/

References to Frameworks to Evaluate Digital Apps or Virtual Platforms Developed in Canada

Quintana, Y, Torous, J. A Framework for Evaluation of Mobile Apps for Youth Mental Health. Homewood Research Institute. May 2020. Available at URL: https://homewoodresearch.org/app-evaluation-project/

Alberta Health Services. (2019). Addiction and Mental Health—Mobile Application Directory 2019. https://www.albertahealthservices.ca/assets/info/res/mhr/if-res-mhr-kt-mobile-app-directory.pdf

Ontario Health, Ontario Telemedicine Network and OntarioMD. Virtual Visits Verification. Available at URL: Verified Solutions | Virtual Visit Solutions for Healthcare Providers.

(CRIC) Canadian Code of Market, Opinion, and Social Research and Data Analytics

A Tool Kit to Enhance the Informed Consent Process for Community-Engaged Pediatric Research

Khanegah, P. (2020). Alberta Rating Index for Apps (ARIA): An Index to Rate the Quality of Mobile Health Applications. Ph.D. Thesis, University of Alberta, Canada. https://doi.org/10.7939/r3-qagm-6984

Mental Health Commission of Canada (MHCC). (2019). Mental Health Apps: How to Make an Informed Choice. Mental Health Commission of Canada (MHCC). https://www.mentalhealthcommission.ca/sites/default/files/2018-01/eMH_app_eng.pdf

Scarborough Health Network. (n.d.). Mental Health App Library – Scarborough Health Network. Retrieved February 15, 2021, from https://www.shn.ca/mental-health/mental-health-app-library/

Strudwick, G., McLay, D., Thomson, N., & Strong, V. (2020). Digital Mental Health Tools: Resources to Support Mental Health Clinical Practice. Centre for Addiction and Mental Health: Toronto, ON. https://infoway-inforoute.ca/en/component/edocman/resources/guides-workbooks/3808-digital-mental-health-tools-resources-to-support-mental-health-clinical-practice

Strudwick G, McLay D, Lo B, Shin HD, Currie L, Thomson N, Maillet É, Strong V, Miller A, Shen N, Campbell J Development of a Resource Guide to Support the Engagement of Mental Health Providers and Patients With Digital Health Tools: Multimethod Study J Med Internet Res 2021;23(4):e25773 doi: 10.2196/25773 PMID: 33885374

Frameworks Developed in the USA

American Psychiatric Association. App Advisor: An American Psychiatric Association Initiative. Available at URL: https://www.psychiatry.org/psychiatrists/practice/mental-health-apps

MindTools. (n.d.). *Mindtools*. MindTools.Io. Retrieved February 15, 2021, from https://mindtools.io/resource-center/

PsyberGuideOneMind. (n.d.). *One Mind PsyberGuide | The Mental Health App Guide Designed with You in Mind*. One Mind PsyberGuide. Retrieved February 15, 2021, from https://onemindpsyberguide.org/

RankedHealth. (n.d.). *Curated Health Apps and Devices*. Retrieved February 15, 2021, from http://www.rankedhealth.com/

Torous, J. B., Chan, S. R., Gipson, S. Y.-M. T., Kim, J. W., Nguyen, T.-Q., Luo, J., & Wang, P. (2018). A Hierarchical Framework for Evaluation and Informed Decision Making Regarding Smartphone Apps for Clinical Care. *Psychiatric Services (Washington, D.C.)*, *69*(5), 498–500. https://doi.org/10.1176/appi.ps.201700423

Frameworks Developed in Europe

NHS. (2021, February 13). *National Health Services. How We Assess Health Apps and Digital Tools*. NHS Digital. https://digital.nhs.uk/services/nhs-apps-library

NHS, England. (n.d.). *Apps and tools for patient care*. NHSX. Retrieved February 15, 2021, from https://www.nhsx.nhs.uk/key-tools-and-info/apps-and-tools-patient-care

COCIR, the European Coordination Committee of the Radiological, Electromedical and Healthcare IT Industry. Market Access Pathways for Digital Health Solutions. November 2020.https://www.cocir.org/fileadmin/Publications_2020/20062_COCIR_Market_Access_Pathways_Digital_Health.pdf

Digital Healthcare Act (Digitale-Versorgungs-Gesetz, DVG) December 2019. Germany https://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl119s2562.pdf stipulates reimbursement criteria for patient-oriented digital health applications (DiGAs) that are Medical Devices of low risk.

Other Frameworks

HealthNavigator, New Zeland. (n.d.). Health Navigator New Zealand. Health Navigator New Zealand. Retrieved February 15, 2021. https://www.healthnavigator.org.nz/apps/m/mental-health-and-wellbeing-apps/

ISO/PRF TS 82304-2. Health software — Part 2: Health and wellness apps—Quality and reliability. https://www.iso.org/standard/78182.html

Lagan S, Sandler L, Torous J. Evaluating evaluation frameworks: a scoping review of frameworks for assessing health apps. BMJ Open. 2021 Mar 19;11(3):e047001. doi: 10.1136/bmjopen-2020-047001. PMID: 33741674; PMCID: PMC7986656.

https://bmjopen.bmj.com/content/11/3/e047001.long

Transparency in Declaration of Conflicts of Interest

Heneghan C, McCartney M. Declaring interests and restoring trust in medicine. BMJ. 2019 Nov 6;367:l6236.. PMID: 31694804 https://pubmed.ncbi.nlm.nih.gov/31694804/

Health On the Net Foundation. Discover the 8 principles of the HONcode in 35 languages. 2019. Available at URL: https://www.hon.ch/cgi-bin/HONcode/principles.pl

Privacy Guidance from Healthcare Applications from Canadian Governments

The Personal Information Protection And Electronic Documents Act ("PIPEDA")
https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/

Canada's Infoway Privacy Guidance Resources
https://www.infoway-inforoute.ca/en/solutions/implementation-support/privacy

Ontario Hospital Association. A Practical Guide to Mental Health and the Law in Ontario. Revised Edition, September 2016. Available at URL:
https://www.oha.com/Legislative%20and%20Legal%20Issues%20Documents1/OHA_Mental%20Health%20and%20the%20Law%20Toolkit%20-%20Revised%20(2016).pdf

Provincial and Federal Guidelines and Laws on Electronic Health Privacy

Privacy Commissioner of Canada. The Personal Information Protection and Electronic Documents Act (*PIPEDA*). Available at URL: https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/

Privacy Commissioner of Canada. PIPEDA in brief
Available at URL: https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda_brief/

Privacy Commissioner of Canada. PIPEDA fair information principles
Available at URL: https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/p_principle/

Information and Privacy Commissioner of Ontario. "Detecting and Deterring Unauthorized Access to Personal Health Information." Jan 28, 2015. Available at URL:
https://www.ipc.on.ca/wp-content/uploads/resources/detect_deter.pdf

Information and Privacy Commissioner of Ontario. Responding to a Health Privacy Breach: Guidelines for the Health Sector. October 2018. Available at URL: https://www.ipc.on.ca/wp-content/uploads/2018/10/health-privacy-breach-guidelines.pdf
https://www.colleaga.org/sites/default/files/attachments/hprivbreach-e.pdf

Information and Privacy Commissioner of Ontario. Privacy and Security Considerations for Virtual Health Care Visits. February 2021. Available at URL: https://www.ipc.on.ca/wp-content/uploads/2021/02/virtual-health-care-visits.pdf

Ontario Government. Personal Health Information Protection Act, 2004, S.O. 2004, c. 3, Sched. A. Available at URL: https://www.ontario.ca/laws/statute/04p03

Privacy Guidelines for Health Care USA

eHealth Initiative (eHI) and the Center for Democracy & Technology (CDT). Proposed Consumer Privacy Framework for Health Data. February 2021. https://cdt.org/insights/cdt-ehis-proposed-consumer-privacy-framework-for-health-data/

Privacy Legislation Europe

The General Data Protection Regulation (GDPR). https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en

The Data Protection Law Enforcement Directive (EU) 2016/680

Peer-Reviewed Publications on Privacy Policies

Robillard JM, Feng TL, Sporn AB, Lai JA, Lo C, Ta M, Nadler R. Availability, readability, and content of privacy policies and terms of agreements of mental health apps. *Internet Interv.* 2019 Mar 6;17:100243. doi: 10.1016/j.invent.2019.100243. PMID: 30949436; PMCID: PMC6430038. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6430038/

Shen N, Bernier T, Sequeira L, Strauss J, Silver MP, Carter-Langford A, Wiljer D. Understanding the patient privacy perspective on health information exchange: A systematic review. *Int J Med Inform*. 2019 May;125:1-12. doi: 10.1016/j.ijmedinf.2019.01.014. Epub 2019 Feb 1. PMID: 30914173. https://www.sciencedirect.com/science/article/pii/S1386505618303009

Shen N, Sequeira L, Silver MP, Carter-Langford A, Strauss J, Wiljer D. Patient Privacy Perspectives on Health Information Exchange in a Mental Health Context: Qualitative Study. *JMIR Ment Health.* 2019 Nov 13;6(11):e13306. doi: 10.2196/13306. PMID: 31719029; PMCID: PMC6881785. Available at URL: https://mental.jmir.org/2019/11/e13306/

Torous J, Roberts LW. Needed innovation in digital health and smartphone applications for mental health: transparency and trust. *JAMA Psychiatry.* 2017;74(5):437–438. doi:10.1001/jamapsychiatry.2017.0262 https://pubmed.ncbi.nlm.nih.gov/28384700/

Parker L, Halter V, Karliychuk T, Grundy Q. How private is your mental health app data? An empirical study of mental health app privacy policies and practices. *Int J Law Psychiatry.* 2019;64:198-204. doi:10.1016/j.ijlp.2019.04.002 https://pubmed.ncbi.nlm.nih.gov/31122630/

Parker L, Karliychuk T, Gillies D, Mintzes B, Raven M, Grundy Q. A health app developer's guide to law and policy: a multi-sector policy analysis. *BMC Med Inform Decis Mak.* 2017;17(1):141. doi: 10.1186/s12911-017-0535-0 https://pubmed.ncbi.nlm.nih.gov/28969704/

Jogova M, Shaw J, Jamieson T. The Regulatory Challenge of Mobile Health: Lessons for Canada. *Health Policy*. 2019;14(3):19-28. https://pubmed.ncbi.nlm.nih.gov/31017863/

Discussion Papers on Electronic Security

Khoo, Cynthia, Kate Robertson, and Ronald Deibert. INSTALLING FEAR. A Canadian Legal and Policy Analysis of Using, Developing, and Selling Smartphone Spyware and Stalkerware Applications By Research report #12, June 2019. https://citizenlab.ca/2019/06/installing-fear-a-canadian-legal-and-policy-analysis-of-using-developing-and-selling-smartphone-spyware-and-stalkerware-applications/

W. Hassan and L. Logrippo, "Towards a process for legally compliant software," *2013 6th International Workshop on Requirements Engineering and Law (RELAW)*, 2013, pp. 44-52, doi: 10.1109/RELAW.2013.6671345. https://ieeexplore.ieee.org/document/6671345

Standards for Electronic Security

Health Information Trust Alliance (HITRUST). https://hitrustalliance.net/

ISO/IEC 27000-series ('ISMS Family of Standards' or 'ISO27K' for short) International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). https://www.iso.org/isoiec-27001-information-security.html

Chartered Professional Accountants of Canada. System and organization controls (SOC) 2 guide: Reporting on controls at a service organization https://www.cpacanada.ca/en/business-and-accounting-resources/audit-and-assurance/internal-control/publications/soc-2-guide