Winter 2022

Policy Document: Health Science Librarians Educational Resource to Assess Privacy Practices of Mental Health Apps

Emily Macleod

Policy Document: Health Science Librarians Educational Resource to Assess Privacy Practices of Mental Health Apps

LIS 9704 Librarianship and Evolving Technologies

Emily MacLeod

December 11, 2022

Health Sciences Library

Policy & Communications Branch

POLICY PRV-001

TITLE: **Mental Health Applications – Performing Privacy Assessments for Healthcare Providers and their Clients**

CATEGORY: **Privacy, mental health applications**

EFFECTIVE: **December 11, 2022**

1.0 SCOPE

1.1 AUTHORITY

The Health Sciences Library has a mandate to provide reference services and educational resources to healthcare providers and their clients. Under the fair information principles, librarians aim to provide accountability among other requirements. The American Library Association also provides a Code of Ethics for librarians to provide a framework to guide ethical decision making in their work.

1.2 **APPLICATION:** This policy applies to librarians providing guidance from a privacy perspective to healthcare providers or patients seeking out mental health apps.

1.3 **PURPOSE:** To provide a coordinated and consistent approach to providing recommendations to healthcare providers and their patients regarding privacy aspects of mental health applications. The purpose of which is to create a general privacy literacy for both audiences when recommending, selecting, and using mental health applications. Building on Becker's statement that 'there are also serious concerns about the privacy of medical records, patients sharing sensitive medical information within these apps, and the potential of inappropriate information sharing,' as well as the American Psychiatric Association's App Advisor model which developed a list of questions that targets key areas of privacy that interrogate a company's privacy and security practices (Becker, 2022, 107-111; American Psychiatric Association, App Advisor).

1.4 BACKGROUND:

In 2022, more than 70% of Canadians believe that they can protect their privacy online but most agreed that they were interested in how their personal information was used, who would be using it or have access to (Canada Health Infoway, 2022, p. 3). As the healthcare system grows to

include telehealth solutions, so too must patients educate themselves on the privacy implications of those solutions. As these solutions collect sensitive personal information, the privacy literacy required to understand what is collected, used, and disclosed becomes a tricky exercise. This also pertains to healthcare providers who often do not have the time to discover the full range of privacy protections offered by mental health apps.

This is true in the mental health space as well. Use of technology to address lack of mental health treatment. With not enough resources, nonprofits and focus groups have stepped up to provide this critical resource. Specifically, the OneMind non-profit organization has created the OneMind Psyberguide to evaluating mental health apps, and the American Psychiatric Association has created the APA App Advisor. While APA provides high level guidance on the questions to ask of mental health apps, OneMind goes a step further to provide recommendations and expert opinions on the apps themselves.

Through an analysis of the OneMind Psyberguide, it was discovered that only 34 of the 265 currently available mental health apps had acceptable privacy policies (OneMind Psyberguide. https://onemindpsyberguide.org/). In order to bridge the gap between the current lack of expert recommendations for mental health apps, health science librarians can educate users to perform their own assessments related to privacy.

1.5 DEFINITIONS

Mental health applications (apps) – applications focused on mental health and behaviour change.

Personal information (PI) – recorded information about an identifiable individual and includes health information

Privacy – the control an individual has over the collection, use, and disclosure of their personal information including health information

Privacy literacy – the level of competence, ability, or knowledge an individual contains around privacy.

Privacy policy: states an organization's position on issues which it has jurisdiction or application over. With respect to privacy, the policy will highlight what information is collected, used, and disclosed by the company. It may also set out the administrative, technical, and physical safeguards, or who individuals may contact should they have questions surrounding the company's information practices.

PRINCIPLES

1. All Health Sciences Library policy requires sign-off by the Head Librarian.
2. All Health Sciences Library policies must fully incorporate fair information principles, where possible.
3. All Health Sciences Library policies must take into consideration the American Library Association's code of ethics.
4. All policy, procedures and guidelines developed must fall in line with current policies, procedures and guidelines and reference them when available.
5. All policy, procedures and guidelines will be structured consistently for general application.
6. Each policy will have an assigned sponsor to coordinate implementation, performance review and to conduct annual reviews.
7. The sponsor is responsible for communicating the policy to staff and for making the policy publicly accessible.

2.0 POLICY STATEMENT

This policy sets out the criteria and process for evaluating mental health apps. It provides guidance and recommendations to health sciences librarians to assist healthcare providers and their patients when they are looking to select mental health applications. Specifically, what is important from the studies, how to contain or mitigate risks when there are no other solutions, or when interoperability forces individuals into one solution over others that may have a better reputation for privacy. This policy includes information for users when interpreting privacy policies such as finding out more about the app, collaborating with others such as IT to build in additional protections; or, seeking out further information from the developer organization responsible for the app.

This policy does not provide recommendations for the use of mental health apps for children or adolescents as the use of mental health apps for these vulnerable populations would require additional considerations (Berger, 2020, 51).

3.0 ROLES AND RESPONSIBILITIES

3.1 Head Librarian

- Acts as a resource for healthcare providers and their patients
- Acts as a sponsor in the policy development process
- Raises awareness of policies both internally among colleagues

and to the public
- Incorporates code of ethics into daily work
- Spearheads initiatives to meet the needs of clients
- Seeks out and leads projects and consults with focus groups to incorporate perspectives into resources

3.2 Librarian
- Acts as a resource for healthcare providers and their patients
- Acts as a sponsor in the policy development process
- Provides feedback to supervisor and team to inform team on trends and share insight
- Tracks review of policy if a policy sponsor

3.3 Healthcare providers
- Provide care and treatment options to patients
- Submit proposals to librarians for reference requests and information
- Share resources with colleagues and patients

3.4 Patients
- Seeks out assistance with reference questions
- Provides data for trends in educational resources or gaps in services

3.5 Developers of mental health applications
- Responsible for ensuring privacy compliance in accordance with applicable legislation
- Communicates to users through privacy policies, terms of use and other methods their information practices
- Raises awareness of changes to clientele
- Maintains technical components of mental health applications
- May work with healthcare providers and patients if developing a solution for a particular set of individuals to incorporate specific technical components or requirements

4.0 ASSESSMENT OF PRIVACY POLICIES

4.1 Identification of a privacy policy

The area of an app where a user will find the organization's information and privacy practices is within its privacy policy. Usually, these are located at the bottom of the homepage for easy accessibility or are included in the 'About' pages of the app.

If an app does not include a privacy policy or one cannot be easily located, users can reach out to the organization to request one. If one does not exist, users should likely look to a different app that provides greater transparency around their privacy practices.

Note: while organizations may make their privacy policies easily accessible, they may not always comply with their stated practices (Iwaya, 2023, p. 6). If there are concerns around how users' personal information is being handled, users can reach out to the organization to request more information (Huckvale, 2019, p. 6).

4.2 Statement of purpose for collecting information

Within the privacy policy, the organization will state the purpose of collecting a users' personal information and how they intend to use that information. The user should be able to read the policy and understand why they are sharing their personal information with the organization. In this way, the privacy policy should be read in clear language at the level of an average individual (Milosevic, 2022, p. 4)

The purpose of collecting personal information must be clear and easily understandable to the user. When personal information is collected for one purpose, it generally cannot be used for another purpose without the consent of the individual. For instance, an organization collects your personal information with consent to use an app, they cannot use your personal information in the future for a marketing campaign unless you have already consented to that use (Huckvale, 2019, p. 6).

4.3 Use of personal health information

In connection with its purpose, the organization should state how it will use the personal information that it collects from its users. It may also collect personal information from other sources about users such as your healthcare provider, if required.

Generally, the use is to provide services to users; however, there may be secondary uses that users are not aware of that may include inventory, training of staff, reporting to professional boards or for testing of the system (Torous, 2019, p. 5).

4.4 Limit or withdrawal of consent procedures

When providing consent for the collection, use and disclosure of personal information, organizations may allow users to place limits on their consent or withdraw their consent going forward. This may be stated at the time that consent is being provided, but if not, users can reach out to the organization to request this (Alqahtani, 2020, p. 2060). In response, the organization may identify that there are unforeseen circumstances that may arise from this limitation or withdrawal of

consent. The user should openly and actively ask questions to the organization to find out how service will be affected.

There may be times that an organization can choose to decline a user's limit or withdrawal of consent. If this occurs, the user is encouraged to seek out the assistance of the Information and Privacy Commissioner/Ombudsman for assistance.

4.5 Third party disclosures

Third party disclosures refer to sharing or releasing personal information from the organization that collected it to another person/organization. The privacy policy may be explicit on what third party disclosures are frequently occurring such as to another IT company for maintenance and support functions of their components. Organizations may also share information with marketing or fundraising companies (Alfawzan, 2022, p.3).

Users should investigate who their personal information is being sent to and if it is not easy to locate, then they reach out to the organization to ask for this information (Alqahtani, 2020, p. 2060).

4.6 Privacy breach protocols

The privacy policy should list the organization's procedure for handling privacy breaches. Specifically, the first step should be for the organization to contain the breach through whatever means necessary to reduce the continued unauthorized use or disclosure of personal information. The second step is for the organization to mitigate the harm caused by the breach by implementing measures to detract from future breaches.

The policy should also indicate when an organization is required to notify users when their personal information has been breached and what is included in that notification. The notification should include the option for the user to make a complaint to the Information and Privacy Commissioner or Ombudsman within their jurisdiction. This office can assist users with understanding their rights in these situations and can also assist organizations when they are handling a breach (Iwaya, 2023).

4.7 Contact individual

The privacy policy should clearly state who the contact individual is for users to contact for more information on their information practices. Oftentimes, the contact individual will be the representative privacy officer, or it may be senior leadership. In either circumstance, the individual must be informed or in a position to answer questions from users (Alfawzan, 2022, p. 2063).

The contact individual may also be responsible for privacy communications and

policies as well as handling privacy breaches and notifying both the individual and Information and Privacy Commissioner/Ombudsman.

4.8 Dissolution of company procedures

In the event that the organization does not continue with providing services, they should have a plan as to where the data is transferred or how it is disposed of. In the case of a dissolution of companies/transfer to new entities, who has ownership of the data and what is the format (ie. is it saved in a format that can only be ready by specialized software?).

In the case of a transfer of ownership, the user should have the opportunity to opt out of the transfer. The best circumstance would be if the organization notified users of the impending transfer and provided a deadline to place opt-out requests.

5.0 PERFORMANCE REVIEW

The policy sponsor will review this policy on an annual basis to assess for currency and to ensure it is relevant to the recommendations being provided to healthcare providers and patients. Policy sponsors may wish to update or amend the policy on a more frequent basis should the need arise.

6.0 APPENDICES

6.1 Appendix A: Privacy Literacy Checklist

VERSION: 1.0

DATE APPROVED: December 11, 2022

APPROVED BY: President,

SPONSOR: Policy Director, Policy & Communications

CONTACT: Policy Director, Policy & Communications (519) 353-3993 KEYWORDS:

privacy, mental health apps

DATE TO BE REVIEWED: December 11, 2023

DATE AMENDED:

Appendix A Privacy Literacy Checklist

As a starting point, users should perform this checklist before providing their personal information to mental health apps. This checklist will be updated as changes are made to the policy. If users have questions that they cannot find the information on their own, they should reach out to the organization requesting their personal information.

☐ The privacy policy is posted on the website and easily accessible to users.

☐ Statement of purpose for collecting information is posted in accessible location for users and the purpose is consistent with the use.

☐ Use of personal information is clear.

☐ Limit or withdrawal of consent is provided in the organization's statement of information practices.

☐ Third party disclosures are clearly included in the privacy policy.

☐ Privacy breach protocols are included within the privacy policy.

☐ Contact Individual: the contact information of an individual at the organization is available to users (likely the Privacy Officer or senior leadership).

☐ Dissolution of company procedures are included within the privacy policy or, can be discovered by contacting the organization.

References

Alfawzan, N., Christen, M., Spitale, G., & Biller-Andorno, N. (2022). Privacy, data sharing, and data security policies of women's mhealth apps: Scoping review and content analysis. *JMIR mHealth and uHealth*, *10*(5), e33735–e33735. https://doi.org/10.2196/33735

Alqahtani, F. & Orji, R. (2020). Insights from user reviews to improve mental health apps. *Health Informatics Journal*, *26*(3), 2042–2066. https://doi.org/10.1177/1460458219896492

American Library Association. (2022). Code of Ethics. https://www.ala.org/tools/ethics

American Psychiatric Association. (2022). App Advisor: An American Psychiatric Association Initiative. https://www.psychiatry.org/psychiatrists/practice/mental-health-apps/app-evaluation-model#privacy

Becker, D.A. (2022). Using mobile mental health apps: An overview. *Journal of Electronic Resources in Medical Libraries*, *19*(3), 107–111. https://doi.org/10.1080/15424065.2022.2113351

Bergin, A. & Davies, E. B. (2020). Technology matters: Mental health apps – Separating the wheat from the chaff. *Child and Adolescent Mental Health*, *25*(1), 51–53. https://doi.org/10.1111/camh.12363

Huckvale, K., Torous, J., Larsen, M.E. (2019). Assessment of the data sharing and privacy practices of smartphone apps for depression and smoking cessation. *JAMA Network Open*, 2(4), e192542–e192542. https://doi.org/10.1001/jamanetworkopen.2019.2542

Iwaya, L. H., Babar, M. A., Rashid, A. & Wijayarathna, C. (2023). On the privacy of mental health apps: An empirical investigation and its implications for app development. *Empirical Software Engineering : an International Journal*, *28*(1), 2–2. https://doi.org/10.1007/s10664-022-10236-0

Kenny, Dooley, B., & Fitzgerald, A. (2016). Developing mental health mobile apps: Exploring adolescents' perspectives. *Health Informatics Journal*, *22*(2), 265–275. https://doi.org/10.1177/1460458214555041

Milosevic, & Pyefinch, F. (2022). Computable consent – From regulatory, legislative, and organizational policies to security policies. In *Enterprise Design, Operations, and Computing* (pp. 3–18). Springer International Publishing. https://doi.org/10.1007/978-3-031-17604-3_1

One Mind Psyberguide. https://onemindpsyberguide.org/

Parker, Bero, L., Gillies, D., Raven, M., & Grundy, Q. (2019). The "hot potato" of mental health app regulation: a critical case study of the Australian policy arena. *International Journal of Health Policy and Management*, *8*(3), 168–176. https://doi.org/10.15171/ijhpm.2018.117

Psihigous, A.M., Stiles-Shields, C. & Neary, M. (2020). The needle in the haystack: Identifying credible mobile health apps for pediatric populations during a pandemic and beyond. *Journal of Pediatric Psychology*, *45*(10), 1106–1113.

https://doi.org/10.1093/jpepsy/jsaa094

Torous, J., Anderson, G., Bertagnoli, A., Christensen, H., Cuijpers, P., Firth, J., Haim, A., Hsin, H., Hollis, C., Lewis, S., Mohr, D., Pratap, A., Roux, S., Sherrill, J., & Arean, P. (2019). Towards a consensus around standards for smartphone apps and digital mental health. *World Psychiatry*, *18*(1), 97–98. https://doi.org/10.1002/wps.20592