ORIGINAL RESEARCH ■ PEER-REVIEWED

Locking it down: The privacy and security of mobile medication apps

Kelly Grindrod, BScPharm, PharmD, MSc; Jonathan Boersema, BA; Khrystine Waked, BSc (AgEnvSc); Vivian Smith, PhD; Jilan Yang, MD, MSc, PhD; Catherine Gebotys, PhD

KELLY GRINDROD

ABSTRACT

Objective: To explore the privacy and security of free medication applications (apps) available to Canadian consumers.

Methods: The authors searched the Canadian iTunes store for iOS apps and the Canadian Google Play store for Android apps related to medication use and management. Using an Apple iPad Air 2 and a Google Nexus 7 tablet, 2 reviewers generated a list of apps that met the following inclusion criteria: free, available in English, intended for consumer use and related to medication management. Using a standard data collection form, 2 reviewers independently coded each app for the presence/absence of passwords, the storage of personal health information, a privacy statement, encryption, remote wipe and third-party sharing. A Cohen's Kappa statistic was used to measure interrater agreement.

Results: Of the 184 apps evaluated, 70.1% had no password protection or sign-in system. Personal information, including name, date of birth and gender, was requested by 41.8% (77/184) of apps. Contact information, such as address, phone number and email, was requested by 25% (46/184) of apps. Finally, personal health information, other than medication name, was requested by 89.1% (164/184) of apps. Only 34.2% (63/184) of apps had a privacy policy in place.

Conclusion: Most free medication apps offer very limited authentication and privacy protocols. As a result, the onus currently falls on patients to input information in these apps selectively and to be aware of the potential privacy issues. Until more secure systems are built, health care practitioners cannot fully support patients wanting to use such apps. *Can Pharm J (Ott)* 2017;150:60-66.

Pharmacists need to pay close attention to the mobile health apps they recommend to patients, especially the privacy and security of apps for medication management.

Les pharmaciens doivent faire très attention aux applications mobiles de santé qu'ils recommandent aux patients, en particulier aux questions de confidentialité et de sécurité liées aux applications de gestion des médicaments.

Introduction

Canadians are moving online and taking personal health information with them. There are more than 165,000 mobile health applications (mHealth apps) on the market, including apps for physical activity, disease management and medication adherence.[1] According to the 2014 National Physician survey, more than 20% of Canada's primary care physicians and 10% of specialists have recommended mHealth apps to patients.[2] Many of the mHealth apps include some aspect of personal health information to help track everything from prescription renewals and medical appointments to blood glucose or activity levels. By using these apps, individuals can update or manage their health status, allowing the health care system to potentially operate more efficiently and cost-effectively. However, health information is highly private and personal and therefore needs to be secured.

Health professionals cannot assume mHealth apps are designed to secure private information. At the individual user level, passwords are an important but not always available feature in mHealth apps. Before health professionals can recommend an mHealth app, we need confirmation that patients can secure their own data reliably and that databases remain secure. Research

DOI:10.1177/1715163516680226

already shows us that inadequate user identification and authentication are major contributors to privacy breaches and data insecurity.[3]

This study analyzes the privacy and security of free medication apps available to Canadians. While apps that help patients manage medications require the input of sensitive information, the privacy and security of those apps have not been clearly explored. Without careful attention to this growing area, Canadians who use medication apps remain at risk of losing privacy in the vital area of their own health care.

KNOWLEDGE INTO PRACTICE

- Health professionals cannot assume mobile health apps are designed to secure private information.
- Of the 184 free medication apps available in Canada, only a third have a privacy policy in place.
- Most free medication apps do not give the user the option to secure the personal health information that they enter into the app.
- Health care professionals and organizations need to put pressure on developers of medication apps to ensure that privacy and security is a priority.

Background

mHealth and medication apps

mHealth is a term increasingly used for health care–related practices supported by mobile technologies. The World Health Organization defines mHealth as a "medical and public health practice supported by mobile devices, mobile phones, patient monitoring applications, personal digital assistants and other wireless devices."[4] The promise of mHealth is that it provides health care professionals, patients, governments and other stakeholders with a new way to use health resources more effectively.

Mobile health and wellness tools are big business. Take the massively popular MyFitnessPal, which was recently sold to the fitness company Under Armour for a reported $475 million (US).[5] At the time of sale, MyFitnessPal had more than 80 million registered users who had used the app or website to track calories consumed and burned throughout the day. The growth in mHealth is also seen in online marketplaces such as Apple's iTunes store, where the number of medical, health and fitness apps grew rapidly, from 9000 apps in 2011 to 43,000 apps in 2013 and then to 165,000 apps in 2015.[1,6,7]

Medication apps include pill reminders, dose trackers, apps for ordering pharmacy refills and medication lists. In 2013, Dayer et al.[8] identified 160 medication adherence apps in the US Apple iTunes and Google Play stores, close to half of which were free. Almost all the apps provided medication reminders and alerts, about a third tracked missed doses and a quarter allowed users to sync or export their personal health data. Considering that an estimated 6% of all mHealth apps now provide medication information or reminders,[1] medication apps are a category needing careful attention.

Regulating medication apps

To complicate matters, mHealth apps such as medication listing or reminder apps fall into a regulatory grey zone. In Canada, medical devices are subject to the Medical Devices Regulation and the Food and Drugs Act.[9,10] Regulated devices are those that help with the diagnosis, treatment, prevention and mitigation of disease (e.g., electrocardiogram), that restore or modify bodily functions or structures (e.g., pacemaker) or that can be used in the diagnosis and care of pregnancy (e.g., pregnancy test). The benefit of regulation is that it dictates how manufacturers must handle complaints, reporting and recalls. The challenge, however, is that in much of the world, the regulations governing medical devices were drafted before the rapid growth of the mHealth industry. This means little to no oversight for the mHealth apps that do not fall easily within the definition of a medical device.

In recent years, regulators such as Health Canada and the U.S. Food and Drug Administration have made clear their intent to regulate only mHealth tools that fit within the traditional definitions of a "medical device," such that the tool is an accessory to a regulated medical device or that it converts a mobile device, such as a smartphone, into a regulated medical device.[11,12] Early examples have included the AliveCor Mobile ECG smartphone case that converts a smartphone into an electrocardiograph and the Withings Wireless Blood Pressure Monitor that converts a smartphone into a blood pressure meter. Meanwhile, medication apps that merely collect or track a user's list of medications fall outside any definition of a medical device and remain unregulated.

MISE EN PRATIQUE DES CONNAISSANCES

- Les professionnels de la santé ne doivent pas supposer que les applications mobiles de santé sont conçues pour sécuriser les renseignements privés.
- Parmi les 184 applications de gestion des médicaments gratuites qui existent au Canada, un tiers seulement disposent d'une politique de confidentialité.
- La plupart des applications gratuites de gestion des médicaments ne donnent pas le choix aux utilisateurs de sécuriser les renseignements médicaux personnels qu'ils entrent dans l'application.
- Les professionnels de la santé et les organisations médicales doivent faire pression sur les développeurs d'applications de gestion des médicaments pour que la confidentialité et la sécurité soient des questions prioritaires.

Keeping medication apps private

Another aspect of regulation is privacy. Medication apps collect sensitive personal health information such as the medications a patient is taking and a record of treatment adherence. Federally in Canada, the Personal Information Protection and Electronic Documents Act (PIPEDA) applies to organizations that are engaged in commercial activities, such as software developers and app developers who collect, use and disclose health information.[13] Exceptions are Ontario, New Brunswick and Newfoundland, which have legislation deemed similar enough to allow for an exemption from PIPEDA. In Ontario, for example, the Personal Health Information Protection Act (PHIPA) outlines how health care professionals, organizations and information technology providers can collect, use and disclose personal health information such as medication information.[14,15]

The challenge of trying to apply legislation such as PIPEDA or PHIPA to an mHealth app is that there is no clear category for mHealth developers, unless the developer has created a product that helps a health information custodian such as a health care professional manage personal health information. The legislation is even less clear when someone downloads an mHealth app from another province or country.[16] The result is that individuals who choose to use an mHealth app like a medication reminder app cannot assume medical device regulations or privacy legislation will protect them.

Locking down medication apps

Although people's awareness of data security is increasing, between 40% and 60% of smartphone users still do not secure their phones, with the most common reasons being to be identifiable to emergency personnel, to allow a lost phone to be returned and because the user believes there is no sensitive data on the phone.[17-19] In fact, since people put personal information on smartphones frequently, that data can be even more valuable—and more vulnerable—than what is on a desktop at home or the office. Most people routinely lock their desktop but do not realize the importance of protecting their smartphone with a simple, 4-digit PIN or passcode. The inclusion of sensitive medication data adds to the need to ensure privacy.

The risks are more than simple speculation. In 2015, Dehling et al.[20] published an analysis of 24,405 health-related apps and identified 12 categories of app risk, with medication apps being at the highest risk of damage due to data leaks, manipulation or loss. Without more transparency, patients and health care providers will not feel confident that medication apps are safe and secure. Thus, we need to mark medication apps as a security priority in the mHealth space. The objective of this study was to examine the privacy and security of medication apps available on the Canadian market to identify areas for improvement.

Methodology

To identify English-language mHealth apps used for medication management, 2 authors (J.B., K.W.) generated a list of apps for review. We searched the Canadian iTunes store for iOS apps using an Apple iPad Air 2 and searched the Canadian Google Play store for Android apps using a Google Nexus 7 tablet. We used the following search terms for both sites: *medication management, medication reminder, pill reminder, medication tracker* and *electronic health record*.

The 2 reviewers downloaded all apps that appeared to be related to medication use onto the study devices. In cases in which an app was available in both iOS and Android, the app was downloaded onto both devices, and differences were noted. We included apps that contained some aspect of personal health information related to medications, were available in English, were intended for consumer use and were available free of charge. We excluded all paid apps and any app that did not contain or imply any personal health information (e.g., an alarm clock app with

TABLE 1 Summary of the privacy and security of free medication apps available in Canada (n = 184)

	Apple iOS apps (n = 93)	**Android apps (n = 91)**	**Total (N = 184)**
Security and privacy features of medication apps			
Password protection available	35 (37.6%)	20 (22%)	55 (29.9%)
Mandatory password	28	15	43
Optional password	7	5	12
Mandatory email and password combination	25	14	39
Medication alerts available	72 (77.4%)	80 (87.9%)	152 (82.6%)
Private alerts (e.g., hidden from lock screen)	11	9	20
Type of information collected by medication apps			
Personal information: name, gender, date of birth	44 (47.3%)	33 (36.3%)	77 (41.9%)
Contact information: address, email, phone no.	29 (31.2%)	17 (18.7%)	46 (25%)
Health information (other than medication names)	82 (88.2%)	82 (90.1%)	164 (89.2%)
Optional provider sharing (e.g., email to provider)	2 (2.2%)	4 (4.4%)	6 (3.2%)
Privacy policies of medication apps			
Privacy policy available	40 (43%)	23 (25.3%)	63 (34.2%)
Encryption of collected information	10	8	18
Remote wipe of collected information	1	0	1
Third-party sharing a possibility	24	11	35
Privacy policy absent	53 (57%)	68 (74.7%)	121 (65.8%)

no medication information). Personal health information, as defined by PHIPA, includes any identifiable information related to the mental or physical health of an individual. In other words, this would entail identifiable information such as a name or email plus medical information such as family health history, doctor's notes, health card number and diagnosed illnesses.[21]

Two authors independently evaluated all downloaded apps using a standard data collection form. We coded for the presence or absence of the following information: privacy policy; encryption; remote wipe; third-party sharing; optional/mandatory password; medication list; medication alerts; alert/reminder privacy; medical conditions; allergies; personal information such as name, gender, date of birth, contact information; health provider name; insurance information; physical measurements such as height, weight or blood pressure; and optional payment. After coding was completed, we measured interrater agreement using Cohen's Kappa statistic.

Results

We identified a total of 455 free apps from the Canadian Apple iTunes store and the Google Play store, including 184 apps that met our inclusion criteria. The ratings agreement was 0.796 and 0.853, for Apple and Android, respectively, with most differences in opinion occurring over interpretations of the privacy policies.

Of the 184 free medication apps evaluated (Table 1), more than two-thirds (70.1%, 129/184 apps) did not have any type of password protection or sign-in system. Of the 29.9% (55/184) of apps that did have some measure of user authentication, we identified 39 that required users to log in using an email and password combination at first use. In addition, of the 184 apps evaluated, 12 apps had the option of turning on a password feature—either as 4-digit PIN or an unrestricted password of the user's choosing (e.g., our default password was "kg").

Most free medication apps had an alert or reminder tool that would help the user with medication adherence. More specifically, 82.6% (152/184) of the apps evaluated had the option of turning on a reminder/alert. Of those 152 apps, 132 had a public alert. This meant that the pop-up was visible on the lock screen and the medication name was displayed. Only 20 had private alerts where the medication name was not displayed or could be changed for privacy.

We also evaluated the apps for the types of information collected, in particular, personal information, contact information and health information. Of the 184 apps evaluated, 41.8% (77/184) requested personal information such as name, gender or date of birth. Moreover, at least 18 apps required this information for the app to function. Contact information (such as address, email or phone number) was requested in 25% (46/184) of apps, being mandatory in at least 4 apps. Health information included insurance number, personal health card number, disease measurements, allergies, conditions and medication names and schedules. The majority (89.1%, 164/184) requested health information other than medication name. In addition, the information collected by these apps can be shared with health care practitioners in 3.2% (6/184) of the apps evaluated, with no information available about the level of security or encryption present during these transfers.

Last, the privacy policies in the evaluated apps were coded for the presence/absence of encryption, remote wipe and third-party sharing. Of the 184 free medication apps evaluated, only one-third (34.2%, 63/184) had a privacy policy available. Within the 63 privacy policies, 18 stated that the information collected by the app would be encrypted, 1 mentioned remote wipe was used for data removal and 35 said the information collected may be shared with third-party companies.

Discussion

More than two-thirds of free medication apps available to Canadians lack basic security measures such as password protection or a privacy policy, despite collecting sensitive personal health information. Even more concerning, while 89% of free medication apps ask for additional health information such as a diagnosis or a disease measure, only 40% ask for identifying information and 19% mention data sharing, raising concerns that many medication apps are actually collecting and sharing data with third parties without user knowledge. Further, only 10% of apps mentioned that the data are encrypted, and only 1 app allowed the user to remotely wipe data in the event of phone loss or theft. One of the most private and secure apps appears to be Pill Manager (Healthnet), which has a mandatory PIN, an alert that can be hidden and a privacy policy stating it is encrypted and has no third-party sharing.

What is most concerning about our findings is that despite the expectation that users will protect their own data, most free medication apps do not give the user the option to secure the personal health information that they enter into the app. The ongoing privacy concerns mean clinicians need to be careful when recommending medication apps to patients, and developers need to step up their game.

Research in the crucial area of mHealth app security and privacy is scant but does support our study's findings. A recent evaluation of Android diabetes apps found that 81% of apps reviewed did not have a privacy policy, slightly higher than our findings of 66%.[22] Similarly, a study of bipolar disorder apps for the Android and Apple devices found that while 50 collected personal data, 76% did not have a privacy policy and only 38% required a user account or password, which was slightly higher than the 30% in our study.[23] Finally, the review by Dayer et al.[8] identified that only 3% of 160 U.S. medication apps were compliant with the U.S. federal privacy legislation known as the Health Insurance Portability and Accountability Act (HIPAA).[8] In the 2014 Global Privacy Enforcement Network sweep of 1211 mobile apps, which included mHealth apps, reviewers found that only 1 in 7 apps offered a clear explanation of how they were collecting, using and disclosing personal health information.[24] Without more transparency, patients and health care providers will not feel confident that medication management apps are safe and secure.

Ideally, all apps that allow users to store medication information will give users the option of securing their data using multifactor authentication through the use of 2 or more authentication options such as a fingerprint with a PIN. Medication apps should include plain-language privacy statements that clearly indicate if data are being shared with third parties and which data. Other important security measures should include remote wipe, encryption, timeouts after a number of unsuccessful authentication tries and secure PIN/password resets. On the back end, sensitive data such as passwords, fingerprints, medication lists and disease markers should also be stored in encrypted (and authenticated) form and made inaccessible to other untrusted/unsecured software. In addition, only hashes of passwords, fingerprint data and patterns locks should be stored for further protection. Cryptographic keys, such as those used for sensitive data encryption, should also be stored securely and generally made inaccessible to users and other untrusted/unsecured software. Finally, medication apps need to support multiparty authentication both on the device and over secure clouds to allow patients control over who may access their data, including clinicians and caregivers.

This study did have its limitations, as it was not feasible to evaluate all medication apps intended for consumer use. We limited our sample group to apps that were available on the Canadian iTunes and Google Play stores, free to use and in English. Hence, other medication apps, including paid apps or apps in another language, may include better security measures and privacy policies. To manage the study's weaknesses, we chose apps from both iOS and Android systems, which allowed us to have a more complete picture of what apps are currently available. We also ensured that the apps downloaded were independently evaluated by 2 authors and that the interrater agreement was measured, strengthening our results. Future research could examine the maximum amount a patient is willing to pay for an app and to assess if paid medication apps have better security measures in place than free apps.

Conclusion

Our medication information, in the wrong hands, has the potential to affect our personal relationships, employment and well-being. Of the 184 free medication apps available in Canada, all contain sensitive medication information, 89% collect additional health information and only a third have a privacy policy in place. Looking to the future, health care professionals and organizations need to put pressure on mHealth developers to build systems that secure medication data. When designed to be secure and private, medication apps have the potential to improve the health of Canadians by improving how we use medications. Until then, it will be very difficult for health care providers to support patients in adopting the growing number of mHealth apps for medication management. ■

From the School of Pharmacy (Grindrod, Boersema, Waked, Yang) and the Department of Electrical and Computer Engineering (Gebotys), University of Waterloo, Waterloo, Ontario; and the University of Victoria (Smith), Victoria, BC. Contact kgrindrod@uwaterloo.ca.

Author Contributions: *K. Grindrod, J. Yang and C. Gebotys conceived of the study design. J. Boersema, K. Waked and J. Yang collected the data. All authors were involved in the data analysis. V. Smith wrote the first version of the article, and all authors provided critical revisions.*

Declaration of Conflicting Interests: *The authors declared no potential conflicts of interest with respect to the research, authorship and/or publication of this article.*

Funding Statement: *This study was funded by a grant from the Office of the Privacy Commissioner of Canada.*

References

1. IMS Institute for Health Care Informatics. *Patient adoption of mHealth: use, evidence and remaining barriers to mainstream acceptance*. Parsippany (NJ): IMS Health; 2015.

2. The College of Family Physicians of Canada. *2014 National Physician Survey*. Toronto (ON): Canadian Medical Association and The Royal College of Physicians and Surgeons of Canada. Available: http://nationalphysiciansurvey.ca/surveys/2014-survey/ (accessed Mar. 16, 2016).

3. Neame RLB. Privacy protection for personal health information and shared care records. *Inform Prim Care* 2014;21:4-91.

4. World Health Organization. *mHealth: new horizons for health through mobile technologies: second global survey on*

eHealth. Geneva (Switzerland): World Health Organization; 2011.

5. De la Merced MJ. Under Armour buys 2 fitness apps, including MyFitnessPal. *New York Times* 2015 Feb. 4.

6. Dolan B. *Mobihealthnews. Report: 13K iPhone consumer health apps in 2012.* Sep. 11, 2011. Available: http://mobihealthnews.com/13368/report-13k-iphone-consumer-health-apps-in-2012/ (accessed Mar. 16, 2016).

7. IMS Institute for Health Care Informatics. *Patient apps for improved health care: from novelty to mainstream*. Oct. 30, 2013. Available: www.imshealth.com/portal/site/imshealth/menuitem.762a961826aad98f53c753c71ad8c22a/?vgnextoid=e0f913850c8b1410VgnVCM10000076192ca2RCRD&vgnextchannel=736de5fda6370410VgnVCM10000076192ca2RCRD&vgnextfmt=default (accessed Mar. 16, 2016).

8. Dayer L, Heldenbrand S, Anderson P, et al. Smartphone medication adherence apps: potential benefits to patients and providers. *J Am Pharm Assoc (2003)* 2013;53:172-81.

9. Government of Canada, Justice Laws Website. *Medical devices regulations (S.O.R./98/282)*. Ottawa (ON): Ministry of Justice. Available: http://laws-lois.justice.gc.ca/eng/regulations/sor-98-282/ (accessed Mar. 16, 2016).

10. Government of Canada. Food and Drugs Act (R.S.C. 1985, c.F-27). Ottawa (ON): Minister of Justice. Available: http://laws-lois.justice.gc.ca/eng/acts/F-27/FullText.html (accessed May 20, 2015).

11. Health Canada. *Notice: software regulated as a class I or class II medical device.* Ottawa (ON): Health Canada; Dec. 3, 2010. Available: www.hc-sc.gc.ca/dhp-mps/md-im/activit/announce-annonce/md_notice_software_im_avis_logicels-eng.php (accessed Mar. 5, 2015).

12. Food and Drug Administration. *Mobile medical applications: guidance for industry and food and drug administration staff.* Silver Spring (MD): Food and Drug Administration; Feb. 9, 2015. Available: www.fda.gov/downloads/MedicalDevices/…/UCM263366.pdf (accessed Mar. 16, 2016).

13. Office of the Privacy Commissioner of Canada. *Provincial legislation deemed substantially similar to PIPEDA*. Available: https://www.priv.gc.ca/leg_c/legislation/ss_index_e.asp (accessed May 20, 2016).

14. Government of Ontario. Personal Health Information Protections Act (S.0. 2004; c.3, Sched A). Jan. 1, 2013. Available: www.ontario.ca/laws/statute/04p03 (accessed Mar. 20, 2015).

15. Cavoukian A. *A guide to the Personal Health Information Privacy Act*. 2004. Available: https://www.ipc.on.ca/images/resources/hguide-e.pdf (accessed Mar. 20, 2015).

16. Hines M. The development of mHealth technology is challenging the effectiveness of current regulation. Gowlings, Nov. 27, 2014. Available: www.lexology.com/library/detail.aspx?g=43f744fd-12e0-465a-9ec8-15ef42cbc4c1 (accessed Oct. 20, 2016).

17. Consumer Reports. 39 percent of smart phone users don't secure their phones. Available: www.consumerreports.org/cro/news/2013/05/consumer-reports-39-percent-of-smart-phone-users-don-t-secure-their-phones/index.htm (accessed Feb. 24, 2015).

18. SOPHOS. 67 percent of consumers don't have password protection on their mobile phones. Aug. 9, 2011. Available: www.sophos.com/en-us/press-office/press-releases/2011/08/67-percent-of-consumers-do-not-have-password-protection-on-their-mobile-phones.aspx (accessed Mar. 16, 2016).

19. Egelman S, Jain S, Portnoff RS, et al. Are you ready to lock? Understanding user motivations for smartphone locking behaviors. CCS '14 Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security. Available: http://dl.acm.org/citation.cfm?id=2660273 (accessed Oct. 24, 2016).

20. Dehling T, Gao F, Schneider S, Sunyaev A. Exploring the far side of mobile health: information security and privacy of mobile health apps on iOS and Android. *JMIR mHealth uHealth* 2015;3(1):e8.

21. Information and Privacy Commissioner of Ontario. *Your privacy rights*. Available: https://www.ipc.on.ca/english/Privacy/Your-Privacy-Rights/ (accessed Mar. 16, 2016).

22. Blenner SR, Kollmer M, Rouse AJ, et al. Privacy policies of android diabetes apps and sharing of health information. *JAMA* 2016;315:1051-2.

23. Nicholas J, Larsen ME, Proudfoot J, Christensen H. Mobile apps for bipolar disorder: a systematic review of features and content quality. *J Med Internet Res* 2015;17(8):e198.

24. Office of the Privacy Commissioner of Canada. From APP-laudable to dis-APP-ointing, global mobile app privacy sweep yields mixed results. Sep. 9, 2014. Available: http://blog.priv.gc.ca/index.php/2014/09/09/from-app-laudable-to-dis-app-ointing-global-mobile-app-privacy-sweep-yields-mixed-results/ (accessed Mar. 16, 2016).