5 Best Practices for Health and Wellness Program Data Security

Cookson James Loyalty
October 2018

ABSTRACT

Trust is a central requirement for any effective health and wellness program. Not only do participants need to feel confident that the program going to help them lead a healthier life, but that their private health information will remain confidential. The more people trust their personal information is protected, the more likely they are to engage in such initiatives fully. In today's hyper-connected world, health and wellness program data are increasingly at risk – whether that be due to internal data mismanagement, the lack of transparency surrounding the selling of data by third-party companies, or external cyber-attacks. In this commentary, the authors explore the importance of health data privacy, as well as the current guidelines and risks associated with the collection and management of health and wellness program user information. It also provides an overview of key best practices that can help support the development of effective health and wellness programs in the workplace and beyond.

INTRODUCTION

Canadians take the privacy and security of their health information seriously. Today's health and wellness programs, whether at the organizational or individual level, collect and manage a tremendous amount of personal information. While these programs offer significant benefits, great care needs to be taken with security as it relates to user data. In light of increasing data breaches, concerns around data security are at all-time high – and the risks are only growing as hackers increasingly target sectors known to store large amounts of personally identifiable information. While Canada just implemented data-breach reporting requirements, as recent as April 2018, U.S. reporting reveals in the last two years that there have been over 400 "large" breaches (500 records or more) of protected health information across the country.[1]

At the same time, digital technology, smartphones and the app economy they've created have led to increasingly comprehensive user surveillance.[2] The more digitized our world becomes, the more susceptible we are to the misuse of our data. Program participants are increasingly realizing their vulnerability. Concerns range from workplace discrimination based on health status, to hackers releasing sensitive information publicly. Privacy has always been a top complaint about mobile apps in general,[3] and mobile health (mhealth) in particular.[4] It's also cited as one of the main barriers to entry for participants in wellness programs,[5] a significant challenge given that the success of

these programs depends on the validity of voluntary user data. With these challenges in mind, this article will examine the current guidelines, risks and best practices for the protection of health and wellness program participant data in Canada.

PRIVACY STANDARDS

When it comes to privacy standards in Canada, there are numerous laws relating to privacy rights and several different organizations and agencies responsible for overseeing compliance. The Office of the Privacy Commissioner of Canada oversees compliance with *The Privacy Act,* which includes the personal information-handling practices of federal departments and agencies, and *The Personal Information Protection and Electronic Documents Act* (PIPEDA), which covers the personal information-handling practices of many businesses.[6] In recent years, the organization has been providing guidance on a variety of technology and privacy topics (including mobile apps[2] and wearables[7]), but health and wellness programs remain largely unregulated in Canada. To further complicate matters, many health and wellness tracker devices are U.S.-based, so any data collected is stored on U.S. servers and fall under different regulations. In the United States, the *Health Insurance Portability and Accountability Act* (HIPPA) applies to only certain "covered entities" that handle personal health information (health care professionals, health insurers, etc.). Data uploaded by citizens to private devices for personal use is a legal grey area. Data protection is governed by the terms of agreement. In addition, given the broad scope of its regulations, the European Union's recent General Data Protection Regulation (GDPR) has major privacy implications for many Canadian organizations such as new consent rules, data subjects' rights and breach notification requirements.

THE RISKS

This combination of rapidly increasing user surveillance and a regulatory grey area leaves wellness program operators open to a variety of challenges. From a workplace wellness program perspective, the collection of health data that is not properly protected could put employees' privacy – and employment – at risk. The selling of data by third-party vendors, medical identity theft and employer discrimination are just a few of the top issues for employees, while legal liability is a major concern for employers. Individuals using health and wellness apps independently may find that these risks are amplified due to the lack of regulation in the health and wellness app space.

Health and wellness mobile apps can be a bit of a perfect storm when it comes to privacy exposure. Studies show again and again that a number of these apps don't meet basic security requirements.[8,9] Many organizations that request to collect sensitive health data from other third-party companies, such as Fitbit, are not sensitized to the handling of such data.[10] The fact that most program users don't take the proper steps to secure their phone only compounds these issues.[11,12]

5 BEST PRACTICES

Given these ever-evolving challenges, health and wellness program facilitators need to invest more in the proper collection and management of user data or ensure that the service providers they choose to deliver their company's health and wellness programs have the appropriate protections in place. Below is an overview of five essential best practices that can help support the development of effective health and wellness programs in the workplace and beyond.

1. **Set clear policies**
    - Have formal policies and procedures in place that are compliant with existing laws and require all employees to abide by them. These policies should give clear direction on what type of user health data is shared, and who that data may be shared with. Standards and appropriate controls must be established to ensure that the electronic exchange or transmission of information is completed in accordance with its classification. This includes appropriate controls and monitoring over the exchange of information with service providers that facilitate health and wellness programs.

2. **Train and test staff**
    - Limit and closely monitor employees and service providers who have potential access to a user's personally identifiable information. Have regular, comprehensive security training and auditing for all staff and vendors who work with wellness program data. Training programs should include policies, standards, requirements, guidelines, responsibilities, related enforcement measures and consequences for non-compliance.

3. **Encrypt and protect data**
    - User verification (i.e., login name and password) should be employed in order for users to access their personally identifiable information or personal health information. To reduce the risk of privacy breaches, devices used to access or share user information should also be equipped with secure encryption software. This will convert user information from a readable state to an unreadable state, an effective method of protecting electronically stored participant information against hackers. In addition, a firewall should be installed between those handling the data and the people making operational decisions.

4. **Physical and environmental security**
    - The physical security of program servers is just as important as online security. Specific measures will depend on facility capabilities but should, at a minimum, include restricting access to servers at the data centre to only a few authorized individuals.

5. **Conduct regular internal policy reviews**
    - Finally, the most important step you can do to protect the privacy of user data is reviewing and auditing your policies and procedures on a regular basis to ensure your staff and service providers are following them. Ensure that the policies, procedures and processes are being followed. A best practice would be to ensure that an independent third-party firm audits security controls and provides a report on audit results. This provides additional legitimacy in the event your compliance efforts are called into question by regulators who may then audit you independently. They can also help provide users with assurance about the confidentiality and privacy of the information processed by your health and wellness program.

QUESTIONS TO ASK

Given what's at stake, it's important to determine privacy capabilities before choosing a health and wellness program provider. Asking a few key questions at the outset can help get your assessment started right. First, what security measures and protocols are in place to meet the latest privacy standards? Find out where the provider's physical servers are and whether any application data is hosted in a cloud service. Second, ask what algorithms are in place to encrypt data and who, if anyone has access to this data? Finally, be sure to ask what security protocols are followed when data is exchanged and whether you can see independent security audits of their data center or hosting facility to ensure they're following industry best practices. While not an exhaustive list, asking for this information early on can help ensure you select a provider capable of protecting your member data now and in future.

CONCLUSION

While it's impossible to guarantee the protection of personally identifiable information and personal health information (there is always some risk that an unauthorized third party may find a way around our security systems or that transmissions of your information over the Internet may be intercepted), taking the steps above will help ensure you're as protected as possible. Trust is a central requirement for an effective wellness program, leading to better outcomes for all. The more people trust their privacy is protected, the more likely they'll engage in health and wellness initiatives and reap the benefits of these essential programs.

REFERENCES

1. U.S. Department of Health and Human Services Office for Civil Rights. (2018, Sept. 20). Breach portal: notice to the Secretary of HHS breach of unsecured protected health information. Retrieved from: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf
2. Office of the Privacy Commissioner of Canada. (2012, Oct.). Seizing opportunity: good privacy practices for developing mobile apps. Retrieved from: https://www.priv.gc.ca/en/privacy-topics/technology-and-privacy/mobile-devices-and-apps/gd_app_201210
3. Khalid, H. et al. (2015). What do mobile app users complain about? *IEEE Software*, *32*(3), 70-77. DOI: 10.1109/MS.2014.50
4. Atienza A, et al. (2015). Consumer attitudes and perceptions on mHealth privacy and security: findings from a mixed-methods study. *Journal of Health Communication*, *20*(6), 673-679. DOI: 10.1080/10810730.2015.1018560
5. Hudson, K. et al. (2017). Undermining genetic privacy? Employee wellness programs and the law. *New England Journal of Medicine*, *377*:1-3. DOI: 10.1080/10810730.2015.1018560
6. Office of the Privacy Commissioner of Canada. (2016, Sept. 9). Privacy laws in Canada. Retrieved from: https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/
7. Office of the Privacy Commissioner of Canada. (2014, July 3). Wearable computing – challenges and opportunities for privacy protection. Retrieved from: https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2014/wc_201401/
8. Grindrod, K. et al. (2018). Evaluating authentication options for mobile health applications in younger and older adults. *PLoS ONE*, *13*(1), 1-16. doi.org/10.1371/journal.pone.0189048
9. Grindrod, K. et al. (2016). Locking it down: the privacy and security of mobile medication apps. *Canadian Pharmacists Journal*, *150*(1), 60-66. doi.org/10.1177/1715163516680226
10. Roosa, S. (2015, Apr. 6). A deep dive into the privacy and security risks for health, wellness and medical apps. Retrieved from Privacy Tech: https://iapp.org/news/a/a-deep-dive-into-the-privacy-and-security-risks-for-health-wellness-and-medical-apps/
11. Smith, A. (2017, Jan. 26). Americans and Cybersecurity. Retrieved from Pew Research Center: http://www.pewinternet.org/2017/01/26/americans-and-cybersecurity/
12. Anderson, M. (2017, March 15). Many smartphone owners don't take steps to secure their devices. Retrieved from Pew Research Center: http://www.pewresearch.org/fact-tank/2017/03/15/many-smartphone-owners-dont-take-steps-to-secure-their-devices/