Unsplash © Onur Binay

Health care apps have a privacy problem

California-based health technology startup myNurse has stopped operating following a major data breach in March that exposed the personal health information of its users. The company, which offered remote patient monitoring services and chronic care management, said the shutdown was "unrelated to the data security incident", but gave no other reason for its decision.

Article originally published on Curation

The breach, which took place on 7 March, saw the personal data of users such as names, dates of birth, medical histories, diagnoses and insurance information accessed by an unauthorised individual. (*TechCrunch*)

Why does this matter?

Health care apps often require sensitive and personal information from individuals in order to operate effectively. It would be expected, therefore, that data of this nature would be protected and securely encrypted to safeguard users, but this is often not the case.

This issue has been thrust into the spotlight once again after the US Supreme

Court’s leaked opinion on the Roe vs. Wade case. There are concerns that period-tracking apps could be used by law enforcement to *target* those suspected of having abortions because, unlike medical records, information gathered by apps is not protected by the Health Insurance Portability and Accountability Act (HIPAA) in the US.

Digital help

Following the COVID-19 pandemic, health care app downloads have increased with mental health apps in particular rising by *200%*.

Growing demand has created a plethora of mental health apps all hoping to capitalise on consumer needs. Pressure to release products, however, may have sidelined privacy details in favour of first-mover advantage.

Not only do certain apps have poor privacy practices, but several, including BetterHelp and Cerebral, claim they reserve the right to *change* policies at any time. Moreover, data can also be passed on to the purchasing company in the case of an acquisition. These incidents aren’t limited to emerging apps or websites – Crisis Text Line has recently stopped sharing conversation data with customer service firm Loris.ai after concerns from data privacy experts.

Negative data

Mental health websites and apps don’t have to sell data to third parties, but many still do. The personal nature of the data is what makes it so *fruitful* for advertisers who can become more targeted in their approach. This method, however, can backfire due to the sensitivity of the information. A bereaved mother, for example, *called out* Facebook, Instagram, Twitter and Experian after she was overwhelmed by baby-related promotions following the death of her child.

Positive data

A lack of transparency and failure to *encrypt* data creates distrust among users and makes it less likely for health care data to be shared when doing so can have *benefits* for treating conditions or furthering research. This suggests there are ways to use data more effectively than just for profit. The prospect of advertising money is an enticing one, however, companies shouldn’t sell sensitive data just because they can.

Fred Fullerton is Senior Sustainability Specialist at *Curation* where this article was originally published

Article by FRED FULLERTON