THE
NATIONAL LAW REVIEW

Pregnancy-Tracking Apps Pose Challenges for Employees

Article By
Adam Jacobson
Risk and Insurance Management Society, Inc. (RIMS)
Risk Management Monitor

- Labor & Employment
- Communications, Media & Internet
- Health Law & Managed Care

- All Federal

Friday, April 26, 2019

As more companies embrace health-tracking apps to encourage healthier habits and drive down healthcare costs, some employees are becoming uncomfortable with the amount and types of data the apps are sharing with their employers, insurance companies and others.

This is especially true for apps that track fertility and pregnancy. As the *Washington Post* recently reported, these apps collect huge amounts of personal health information, and are not always transparent about who has access to it. The digital rights organization Electronic Frontier Foundation even published a paper in 2017 titled *The Pregnancy Panopticon* detailing the security and privacy issues with pregnancy-tracking apps. Employers can also pay extra for some pregnancy-tracking apps to provide them with employees' health information directly, ostensibly to reduce health care spending and improve the company's ability to plan for the future.

Given the documented workplace discrimination against women who are pregnant or planning to become pregnant, users may worry that the information they provide the apps could impact employment options or treatment by colleagues and managers.

Pregnancy-tracking apps also collect infinitely more personal data than traditional health-tracking apps and devices like step-counters or heart rate monitors. This can include everything from what medications users are taking and when they are having sex or their periods, to the color of their cervical fluid and their doctors' names and locations.

Citing discomfort with providing this level of information, the *Washington Post* reported some women have even taken steps to obscure their personal details when using the apps, for fear that their employers, insurance companies, health care providers or third parties may have access to their data and could use it against them in some way. They use fake names or fake email addresses and only give the apps select details or provide inaccurate information. Fearing the invasion of their newborn children's privacy, some have even chosen not to report their children's births on the apps, despite this impacting their ability to track their own health and that of their newborn on the app.

Like many other apps or online platforms, it may be difficult to parse out exactly what health-tracking apps are doing with users' information and what you are agreeing to when you sign up. When employers get involved, these issues get even more difficult. By providing incentives—either in the form of tangible rewards like cash or gift cards, or intangible benefits such as looking like a team player—companies may actually discourage their employees from looking closely at the apps' terms of use or other key details they need to fully inform the choice to participate or not.

While getting more information about employees' health may offer ways to improve a workforce's health and reduce treatment costs, companies encouraging their employees to use these apps are also opening themselves up to risks. As noted above, apps are not always transparent as to what information they are storing and how. Depending on the apps' security practices, employees' data may be susceptible to hacking or other misuse by third-party or malicious actors. For example, in January 2018, fitness-tracking app Strava released a map of users' activity that inadvertently exposed sensitive information about military personnel's locations, including in war zones. Given the kinds of personal details that some apps collect, health app data could also put users at risk of identity theft or other types of fraud.

Tracking, storing, and using workers' personal health information also exposes employers and insurance companies to a number of risks and liabilities, including third-party data storage vulnerabilities and data breaches. This is especially important in places governed by stringent online data protection regulations like the European Union's General Data Protection Regulation (GDPR). In addition to the risks of reputation damage, companies that are breached or otherwise expose employees' personal information could face significant regulatory fines.

People using health-tracking apps, especially fertility-related apps, should weigh the costs and benefits of disclosing personal information against how apps and others are using this information. Companies who encourage their employees to use these apps and collect their personal health details should also be as transparent as possible about how they are using it, and implement measures to protect workers' personal data to the fullest extent possible and ensure that managers are not using this data to discriminate against workers.

Risk Management Magazine and Risk Management Monitor. Copyright 2019 Risk and Insurance Management Society, Inc. All rights reserved.

Source URL: https://www.natlawreview.com/article/pregnancy-tracking-apps-pose-challenges-employees