

Cardiologists: Big data advances research, but shouldn't do so at the cost of privacy

February 24 2020



Health data collected from your apps or wearable devices could revolutionize personalized health care, but the current lack of legal protections related to this technology could lead to personal health information becoming available to unscrupulous third parties, according to a new publication in *Circulation*. Credit: Michigan Medicine

We know we shouldn't, but most of us have clicked "agree" in a hurry to download an app or sign up for a streaming service without reading the

user agreement in detail.

And it might seem pretty safe to add an app that promises to help take control of your [health](#) through simple things like tracking your steps, measuring your blood pressure or noting your eating and exercise habits. But doctors who appreciate the research potential of incorporating [big data](#) into [medical care](#) are also warning about the need to manage the risk of exposing such health data while it's still possible to do so.

That's because the average patient probably has no idea about the complex rules around what happens to their sensitive health data when it is collected by apps. For instance, a 2019 study found 19 out of 24 health-related apps studied shared their users' data. Patient privacy laws preclude providers from sharing information, but the commercially available apps used to collect it don't necessarily have to follow HIPAA, the law that governs privacy about [health information](#).

"Some health data shared with a physician in the context of a health-related interaction is protected, but in a different context that same data is not protected," says Jessica Golbus, M.D., a cardiovascular medicine fellow at the Michigan Medicine Frankel Cardiovascular Center. "The way the U.S. addresses health data focuses on who is using the data, but not the data itself."

This lack of protection could lead to people's sensitive data becoming available to unscrupulous third parties with sales interests, or those making decisions about life or disability insurance or employment, she says.

She authored a new perspective to highlight these consequences, published in the February 25 issue of *Circulation*, with two members of the University of Michigan's Institute for Healthcare Policy & Innovation: Brahmajee Nallamothu, M.D., MPH, also with the Frankel

CVC, and W. Nicholson Price II, J.D., Ph.D., also with the U-M Law School.

Benefits outweigh risks—so far

Imagine getting a [text message](#) on a sunny day to remind you to go for a walk if you're trying to keep up your momentum after cardiac rehab, or a notification popping up with a sleep tip if your smartwatch finds you haven't gotten enough ZZZ's this week. Without advanced consumer devices that allow for data collection and synthesis, these kinds of interactions would still be a faraway dream. But these interventions are already here, or just around the corner.

And they have the potential to help patients better manage their own health, the authors believe.

"We're learning how to leverage [digital technology](#), like smartphones and wearables, to engage patients in their health, improve remote monitoring of health conditions and potentially deliver targeted interventions outside of the clinic appointment," Golbus says.

The authors say they don't want to scare patients or providers away from embracing these potential improvements to research and [patient care](#), because the benefits presently outweigh the risks. However, the risks of commercial exploitation and privacy harms should be addressed, they write.

"We simply think it's important to make sure providers who are encouraging their patients to use this technology are also able to have conversations with their patients about data privacy," Golbus says.

The need for education and advocacy

Golbus and colleagues suggest urgently addressing two areas: provider education and legislation. This, they believe, would help researchers continue to harness more data than they've ever had access to before to improve health and disease prevention and treatment, while also protecting their patients' privacy.

"It could be helpful for patients to provide doctors with their heart rate and blood pressure measurements collected using wearable devices," co-author Nallamothu added. "But this means we have a responsibility to educate patients and ourselves about potential downstream uses of that data."

This is a problem that will be difficult for consumers to solve on their own, the authors say.

As in many other commercial areas, data are being collected at large scale with little understanding by the public. Beyond the need for health care providers to learn about and raise awareness of the risks to using commercially available applications, the authors say the government should also ensure better protection of consumer data.

The responsibility shouldn't be placed only on the shoulders of consumers worrying about to whom they've consented to data sharing, they write.

"The U.S. is living in the past with regard to data protection," co-author Price says. "We've got privacy law from a world where health data means what your doctor writes in your medical chart. We're not in that world anymore. The law needs to change."

More information: Jessica R. Golbus et al, Privacy Gaps for Digital Cardiology Data, *Circulation* (2020). [DOI: 10.1161/CIRCULATIONAHA.119.044966](https://doi.org/10.1161/CIRCULATIONAHA.119.044966)

Provided by University of Michigan

Citation: Cardiologists: Big data advances research, but shouldn't do so at the cost of privacy (2020, February 24) retrieved 12 May 2024 from

<https://medicalxpress.com/news/2020-02-cardiologists-big-advances-shouldnt-privacy.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.