Health Gadgets and Apps Outpace Privacy Protections, Report Finds

July 19, 2016

The federal patient privacy law known as HIPAA has not kept pace with wearable fitness trackers, mobile health apps and online patient communities, leaving a gaping hole in regulations that needs to be filled, according to a much-delayed government report released today.

The report, which was supposed to be complete in 2010, does not include specific recommendations for fixing the problem, even though Congress asked the U.S. Department of Health and Human Services to provide them.

HHS' findings largely mirror those in a ProPublica story from last November. The Health Insurance Portability and Accountability Act, the landmark 1996 patient-privacy law, only covers patient information kept by health providers, insurers and data clearinghouses, as well as their business partners. Falling outside the law's purview: wearables like Fitbit that measure steps and sleep, at-home paternity tests, social media sites, and online repositories where individuals can store their health records.

"Health privacy and security law experts have a reasonably clear idea of where HIPAA protections end, but the layperson likely does not," said the report written by HHS'

Office of the National Coordinator for Health Information Technology, in conjunction with other agencies. "Moreover, even entrepreneurs, particularly those outside the health care industry 2026 may not have a clear understanding of where HIPAA oversight begins and ends."

The report was mandated under a 2009 law that called on HHS to work with the Federal Trade Commission 2014 which targets unfair business practices and identity theft 2014 and to submit recommendations to Congress within a year on how to deal with entities handling health information that fall outside of HIPAA. Asked why the report did not include any recommendations, an official said readers could draw their own conclusions from the findings.

"At the end of the day, it's a very complicated environment that we find ourselves in," said Lucia Savage, chief privacy officer at the Office of the National Coordinator for Health Information Technology, which took the lead on the report. "We believe we're fulfilling our duties. If Congress has concerns about that, I'm sure that we will hear about them."

In 2013, the Privacy Rights Clearinghouse studied 43 free and paid health and fitness apps. The group found that some did not provide a link to a privacy policy and that many with a policy did not accurately describe how the apps transmitted information. For instance, many apps connected to third-party websites without users' knowledge and sent data in unencrypted ways that potentially exposed personal information.

Paul Stephens, the group's director of policy and advocacy, said the issue has grown more urgent in recent years as employers give workers incentives to log their activities on mobile apps as part of wellness programs. "It goes beyond someone voluntarily saying I want this app," Stephens said. "There are basically going to be financial incentives to use the app."

Stephens also said many people do not read an app's privacy policy, leaving them open to having their information used in myriad ways.

The new report pointed to a number of major differences between information covered by HIPAA 2014 your medical records, for instance 2014 and data that's not. Among them:

- Under HIPAA, patients are entitled to copies of their health records. Companies that make trackers and apps "are not obligated by a statute or regulation to provide individuals with access to data about themselves."
- HIPAA delineates to whom and for what purpose a health provider may share a patient's health information and limits the use of personal health information for marketing. People who have provided information to companies that fall outside the law "likely will not enjoy the same protections against unwanted marketing unless the data collector has promised in its terms of use not to use data for marketing and does not change its terms of use."
- HIPAA rules require tight security over personal health information. Apps and wearables may not have the same protections.

- HIPAA requires understandable privacy policies and notices. Outside the law, those may not exist.

In addition, several federal agencies have a role in regulating privacy, new technology and consumer protections. The HHS Office for Civil Rights enforces HIPAA; the FTC acts against deceptive or unfair trade practices; and the Office of the National Coordinator encourages adoption of health information technology.

A 2014 study looked at 600 of the most commonly used health apps and found that fewer than a third had privacy policies. And for those that did, you'd have to have the reading level of a college senior to understand them, the HHS report said. Policies on Apple and Google mobile phone platforms "may be inconsistent, not articulated to individuals, or simply ignored by web developers skirting the rules that operating system developers attempt to impose on them."

Attempts to fix the problem through voluntary efforts do not appear to be working. In 2015, the Consumer Electronics Association issued a set of "Guiding Principles on the Privacy and Security of Personal Wellness Data."

"These guidelines *can* be adopted by companies, but are not required of CEA members," today's report said. "As of July 2016, we have been unable to identify any companies that have adopted the guidelines."

The report offers no suggestions to change that, either.

This article was originally published on ProPublica, a Pulitzer Prize-winning investigative newsroom. Sign up for their newsletter .

http://www.govtech.com/applications/Health-Gadgets-and-Apps-Outpace-Privacy-Protections-Report-Finds.html