How Private Is Your Health Data?

By Stephanie Watson
Medically Reviewed by Michael W. Smith, MD
June 24, 2021

Many of the health monitoring activities we used to do in our doctor's office have moved into the digital world. Smart watches and apps track our sleep, workouts, diet, and stress levels. We use online portals to check test results, refill prescriptions, and make doctor's appointments.

Having so much personal health information floating around in cyberspace raises important privacy issues. Just who has access to our digital health data, and what could they do with it?

Although nearly two-thirds of Americans say they like being able to manage their health on their devices, most are concerned about the security of their personal data.

Though there's good reason to worry, there are also ways to protect your digital health data.

HIPAA and the Privacy of Your Health Data

The Health Insurance Portability and Accountability Act (HIPAA) is a federal law signed in 1996 to protect the security of personal health information. HIPAA prevents doctors, hospitals, and insurance companies from releasing your private health data without your permission.

Most health plans and health care providers that are governed by HIPAA have safeguards in place "to ensure the confidentiality, integrity, and security of individuals' information," says Maria Garcia, JD, partner and co-chair of the Healthcare Practice at Kozyak, Tropin, & Throckmorton, a law firm in Coral Gables, FL.

The trouble with HIPAA is that it was written years before health apps and other digital health information-sharing tools became commonplace. HIPAA protects the digital information that's stored in your electronic health record (EHR), including your medical history, diagnoses, medications, and test results. Your EHR is stored in a digital database accessible to you and your doctors and hospitals, but it is ultimately under your control. HIPAA doesn't cover the health information you share over mobile apps or social media websites.

"HIPAA is grossly outdated," says Brendan Parent, JD, director of Transplant Ethics and Policy Research, and assistant professor of Bioethics and Surgery at the NYU Grossman School of Medicine. "It assumed that how data is created and who is using it are the only things that matter in terms of how it needs to be protected."

How Safe Is Your Digital Health Information?

Health data is "gold," Parent says. With so much health information available online, it was only a matter of time before someone tried to exploit it for profit.

In the second half of 2020, hackers broke into more than 21 million patient records, up 177% from just a few months earlier. More than 90% of health care organizations have reported at least one data breach over the last 2 years.

Once hackers gain access, they hold patient information for ransom, vowing to release names, diagnoses, and other sensitive information if hospitals don't meet their demands for money.

Far less sinister but also worrisome are the health tracking apps where people share all kinds of personal health information. Though there isn't much risk in revealing the number of steps you walk each day, sharing information about your menstrual cycle or mental health could be a problem. "These are the sorts of things that many people are, frankly, giving up for free," says Nicholson Price, JD, PhD, professor of law at Michigan Law.

What Kinds of Health Information Do Companies Collect?

Many of us quickly click through the pages of terms and conditions that detail how a tech company plans to use our health information. And even if we did read the fine print, we might not get the whole story.

In one study, 83% of diabetes apps that researchers tested had privacy policies for how they gather, store, and use their customers' personal information. But all of them shared that data with other companies, often without their customers' knowledge.

We also reveal personal information on our social media pages. "Even a single tweet or Facebook post that seems on its surface to have no relationship to our personal health and well-being, such as 'I went to the club and enjoyed this song,' can be correlated with other pieces of information that could have consequences for your health," Parent says.

Those additional pieces of information might come from your EHR, released by your doctor for the purpose of medical research. HIPAA requires that your data first be stripped of 18 key pieces of information that could be used to identify you, like your name, address, and Social Security number.

But using technologies like artificial intelligence and machine learning, computers can now track you down, even without these data points. "With the advent of big data and artificial intelligence, it's a lot easier to take a lot of disparate pieces of information and put them together into one big picture," Price says.

Worst-case scenario, a hacker could get access to important details about your medical history and threaten to expose them if you don't pay up. More likely is that a company will sell your health information. Although your medical history technically can't be used to discriminate against you, in theory, a life insurance company could buy it and then use it to "jack up your insurance rates," Parent adds.

How to Protect Your Health Data

Some states are getting tougher on companies that use personal health data. The California Consumer Privacy Act gives consumers the right to know what personal information companies collect on them, and to delete that information or prevent it from being sold.

No matter where you live, ultimately you are the primary guardian of your own digital health information. Price says he doesn't have any health apps on his phone. "Part of that is because I'm not clear on exactly how my data will or might be used," he says.

If you do intend to share health information electronically, use caution. Create a strong password -- one that contains letters, numbers, and symbols -- to protect people from getting access through your phone or computer.

Only buy health tech and apps from trusted sources, and read the fine print. Review the company's privacy policy and terms of service to learn what types of health information it will collect, and how it plans to use and share it. You do have the right to opt out of data sharing, although the trade-off is that it could affect the app's functionality, Parent says.

Finally, think before you post. Don't put any health information on social media that you wouldn't want anyone -- and everyone -- to read.