Our laws don't do enough to protect our health data

October 23 2017, by Sharona Hoffman

Credit: AI-generated image (disclaimer)

Have you ever wondered why your computer often shows you ads that seem tailor-made for your interests? The answer is big data. By combing through extremely large datasets, analysts can reveal patterns in your behavior.

A particularly sensitive type of [big data](#) is medical big data. Medical big data can consist of [electronic health records](#), insurance claims, information entered by patients into websites such as [PatientsLikeMe](#) and more. Health information can even be gleaned from web searches, Facebook and your recent purchases.

Such data can be used for [beneficial](#) purposes by medical researchers, public health authorities, and healthcare administrators. For example, they can use it to study medical treatments, combat epidemics and reduce costs. But others who can obtain medical big data may have more selfish agendas.

I am a professor of law and bioethics who has researched big data extensively. Last year, I published a book entitled [Electronic Health Records and Medical Big Data: Law and Policy](#).

I have become increasingly concerned about how medical big data might be used and who could use it. Our laws currently don't do enough to prevent harm associated with big data.

What your data says about you

Personal health information could be of interest to many, including employers, financial institutions, marketers and educational institutions. Such entities may wish to exploit it for decision-making purposes.

For example, employers presumably prefer healthy employees who are productive, take few sick days and have low medical costs. However, there are laws that prohibit employers from discriminating against workers because of their health conditions. These laws are the [Americans with Disabilities Act](#) (ADA) and the [Genetic Information Nondiscrimination Act](#). So, employers are not permitted to reject qualified applicants simply because they have diabetes, depression or a

genetic abnormality.

However, the same is not true for most predictive information regarding possible future ailments. Nothing prevents employers from rejecting or firing healthy workers out of the concern that they will later develop an impairment or disability, unless that concern is based on genetic information.

What non-genetic data can provide evidence regarding future health problems? Smoking status, eating preferences, exercise habits, weight and exposure to toxins are all [informative](#). Scientists believe that [biomarkers](#) in your blood and other health details can [predict cognitive decline, depression and diabetes](#).

Even bicycle purchases, credit scores and voting in midterm elections can be [indicators](#) of your health status.

Gathering data

How might employers obtain predictive data? An easy source is social media, where many individuals publicly post very private information. Through social media, your employer might learn that you smoke, hate to exercise or have high cholesterol.

Another potential source is [wellness programs](#). These programs seek to improve workers' health through incentives to exercise, stop smoking, manage diabetes, obtain health screenings and so on. While many wellness programs are run by third party vendors that promise confidentiality, that is [not always the case](#).

In addition, employers may be able to purchase information from [data brokers](#) that collect, compile and sell personal information. Data brokers mine sources such as social media, personal websites, U.S. Census

records, state hospital records, retailers' purchasing records, real property records, insurance claims and more. Two well-known data brokers are [Spokeo](link) and [Acxiom](link).

Some of the data employers can obtain identify individuals by name. But even information that does not provide obvious identifying details can be valuable. Wellness program vendors, for example, might provide employers with [summary data](link) about their workforce but strip away particulars such as names and birthdates. Nevertheless, de-identified information can sometimes be [re-identified by experts](link). Data miners can match information to data that is publicly available.

For instance, in 1997, Latanya Sweeney, now a Harvard professor, famously [identified](link) Massachusetts Governor William Weld's hospital records. She spent $20 to purchase anonymized state employee hospital records, then matched them to voter registration records for the city of Cambridge, Massachusetts.

Much more sophisticated techniques now exist. It's conceivable that interested parties, including employers, will pay experts to re-identify anonymized records.

Moreover, de-identified data itself can be useful to employers. They may use it to learn about disease risks or to develop profiles of undesirable employees. For example, a Centers for Disease Control and Prevention [website](link) allows users to search for cancer incidence by age, sex, race, ethnicity and region. Assume employers discover that some cancers are most common among women over 50 of a particular ethnicity. They may be very tempted to avoid hiring women that fit this description.

Already, some employers refuse to hire applicants who are [obese](link) or [smoke](link). They do so at least partly because they worry these workers will develop health problems.

What's stopping them?

So what can be done to prevent employers from rejecting individuals based on concern about future illnesses? Currently, nothing. Our laws, including the ADA, simply do not address this scenario.

In this big data era, I would urge that the law be revised and extended. The ADA protects only those with existing [health problems](link). It's now time to begin protecting those with future health risks as well. More specifically, the ADA should include "individuals who are perceived as likely to develop physical or mental impairments in the future."

It will take time for Congress to revisit the ADA. In the meantime, be careful about what you post on the internet and to whom you reveal [health](link)-related information. You never know who will see your data and what they will do with it.

This article was originally published on [The Conversation](link). Read the [original article](link).

Provided by The Conversation