Third Parties and Your Health Data: What's the Fine Print?

Save to myBoK

By Mary Butler

Wellness-obsessed consumers now have more tools at their disposal than ever before to help them "live their best lives," as Oprah might say.

While employer-sponsored health insurance helps individuals gain access to access to care, employer-provided wellness programs can help health maintenance by offering discounted or free gym memberships and other perks such as smoking cessation classes. As the *Harvard Business Review* reported, two-thirds of United States-based employers offer wellness programs of some kind, and a majority of those offer an incentive, such as reduced insurance premiums, to get more employees on board. Participants in these programs may also be using tools such as MyFitnessPal and wearable health trackers like FitBits.

For a certain segment of the population, these tools aren't enough. People with family histories of certain cancers and genetic diseases are increasingly investing in DNA analysis—whether it's testing done in their doctor's office or through online testing services such as AncestryDNA, 23andMe, National Geographic, and others.

But all of these technologies require the exchange of sensitive information—the protection of which consumers too frequently overlook when they sign up for these online services and devices.

"There are all kinds of places that are creating, storing, holding, using your health information that aren't covered by HIPAA," said Kirk Nahra, JD, a partner at the law firm Wiley Rein. He notes that consumers with even a basic understanding of HIPAA don't understand the difference between protections provided by HIPAA-covered entities and the protections offered to consumers by federal regulators and the individual 23andMe and AncestryDNA privacy policies. "That's clearly a problem with the law. And… there's a lot of discussion about whether we need to do something about that."

Read the Fine Print

Several recent news articles have highlighted the risks of failing to read the privacy agreements that come with direct-to-consumer DNA testing services—AncestryDNA and 23andMe in particular.

An article in *Forbes* points out that 23andMe "has sold access to its database to at least 13 outside pharmaceutical firms. One buyer, Genentech, ponied up a cool $10 million for the genetic profiles of people suffering from Parkinson's. AncestryDNA, another popular personal genetics company, recently announced a lucrative data-sharing partnership with the biotech company Calico."

The author of the *Forbes* article, former FDA associate commissioner and president of the Center for Medicine in the Public Interest, Peter Pitts, argues that the data collected by AncestryDNA and 23andMe, in addition to being sold to companies that may not completely anonymize the data, is vulnerable to hacking attempts.

"Once genetic data has been linked to a specific person, the potential for abuse is vast and frightening. Imagine a political campaign exposing a rival's elevated risk of Alzheimer's. Or an employer refusing to hire someone because autism runs in her family," Pitts posits.

But Nahra is skeptical of these types of claims. The Genetic Information Nondiscrimination Act (GINA) prohibits the type of discrimination Pitts is concerned about. And, as Nahra notes, it's not clear that genetic information is valuable to a hacker.

"There's a rational uneasiness about the unknown," Nahra said. "…you can't commit identity theft because you have a DNA sample. You can't get access to my health insurance because you have a DNA sample. But we also don't know what else

there is. There clearly are concerns about insurance companies using genetic information, but there are laws on that right now," Nahra said, referring to GINA.

He added that if there's a data breach at one of these DNA companies, the Federal Trade Commission (FTC) can take action.

But the standard for FTC action comes if a company's policies are deemed unfair and deceptive.

For example, Nahra says that if one of these companies writes into their privacy policy that "if you utilize our services, we reserve the right to put your information on a billboard so anybody in the world can read it," is the FTC going to have a problem with that and what's their vehicle for finding a problem for that?" Nahra asks. "Is that unfair and deceptive practice? It's not deceptive because they told you about it. The question is: is that inherently unfair? And the FTC hasn't pushed that yet. So we don't know if the FTC is in fact going to create any boundary lines on that."

Workplace Wellness Programs

Employee wellness programs look like a win-win for everyone involved. If employees take advantage of the perks of their company's initiatives—weight loss programs, gym memberships and discounts, or even things like free yoga classes—their overall health can improve. This also saves the employer's insurance company some money.

However, a recent article in the *Harvard Business Review* notes that things can get dicey because the vendors some employers rely on for wellness programs are—like the DNA testing companies—often storing large amounts of sensitive data. Once again, these vendors aren't necessarily HIPAA-covered entities.

"Often employees are not informed before joining a wellness program that vendors may sell the health information they collect. This does not appear to be well-known among employers, either. Some vendors are for-profit entities and are not connected to a health insurance carrier, which means that much of the information their programs collect exists in a legal gray area, since that information is not protected by laws such as the Health Information Portability and Accountability Act (HIPAA)," the *Harvard Business Review* reports.

The article goes on to note that while laws like GINA and the Americans with Disabilities Act prohibit employers from discriminating against employees, "the health data collection that's part of workplace wellness programs may put employees' privacy, and potentially even employment, at risk."

Again, the onus falls to the employer as well as individuals to read every document they sign where their own health information is at stake.

"Employees who wish to join a workplace wellness program should carefully read the consent forms for health data collection and make sure they understand what data will be collected and how it will be used—both by the third-party vendor and by the employer," the article states. "Employees should demand assurances from their employer that their health data won't affect any employment decisions."

Mary Butler is the associate editor at *The Journal of AHIMA*.

Original source:
Butler, Mary. "Third Parties and Your Health Data: What's the Fine Print?" (Journal of AHIMA website), July 01, 2017.
