

Need medical help? Sorry, not until you sign away your privacy

When you're sick, you're vulnerable—and that's when your doctor pressures you into participating in a data-gathering experiment.

by **Mary Madden**

Oct 23, 2018

Last summer I found myself running late for a doctor's appointment I'd waited months to get. Even though the back injury I had sustained three months earlier was finally starting to improve, I was eager to get an expert opinion from an orthopedic surgeon. When I arrived, breathless and apologetic, the doctor's office was filled with patients—many with much more serious injuries than mine—who had also waited months to see the renowned specialist. As I was about to take my seat, I was called back to the front desk: Could I also please answer some questions about my personal health history using the office's new tablet-based system?

As a social science researcher who has studied digital privacy and security issues for much of my career, I was less than thrilled to be a guinea pig for their new data-management system. But ... I had waited so long for this appointment, and I had already kept the doctor waiting, and maybe this would save me time at future appointments with other doctors? At that moment, as if in response to my frustrated realization that there was no clear way to opt out and still receive the care I needed, my back muscles tightened up.

I nodded politely and brought the tablet back to my chair. From the institutional perspective, this was a totally reasonable request for verification. But it was also a clear instance of surveillance, and the power dynamics between me and the administrative authority were not at all equal. I was in pain and in no mood to argue.

By agreeing to use the tablet, I'd already consented to a form of data collection I wasn't entirely comfortable with. I had never heard of the branded tablet the office was using, and the logo assuring me that it was "antibacterial" didn't ease my concerns about letting scores of other patients handle a device into which I'd put my private data. The awkward software interface did little to suggest that my data would be dealt with carefully; worse than the clunky visual design, there was no indication of whether or not the tablet was internet-connected, and there was no explanation of how my data would be stored or protected once it entered their system.

So what did I do? I dutifully entered my info anyway—immediate physical needs have a way of leapfrogging over data privacy concerns, even for people like me who feel strongly about maintaining control over how their information is collected and used.

Not the first time this happened

As I scrambled to consult my phone for records of my grandparents' cause of death and the appropriate medical term to describe the blood condition that runs in my family, I realized that this was probably the fourth time over the past year that I'd been asked to enter some version of this data digitally in other systems—in addition to various paper versions of the same information. Instead of making the patient experience more efficient and less stressful, it made me feel as though doctor's offices were crowdsourcing their work to stressed-out patients with little explanation of why.

When I'd finished digitally detailing my health history, the final screen seemed to mock me with one last request: Could I please acknowledge that I'd received a copy of the office's privacy practices? (I hadn't.) But what were the consequences of opting out at this point? And what about people who were much less comfortable with technology than I was? How were they dealing with questions or concerns about this process?

The banality of Big Brother

In the internet age, it's become repetitive and banal to simply agree to terms of service that we don't fully understand. And while it would be nice to think that my doctors and their third-party software vendors will forever treat my health data with the utmost care, the reality is that digital health data systems have been vulnerable to numerous ransomware attacks, genetic testing companies have opened up their customers' data to use by pharmaceutical companies, and the market for health data is massive and growing.

I've spent more than a decade studying Americans' attitudes to different kinds of digital information, and I have seen repeatedly that health data is one of the most sensitive categories. In a study I contributed to at the Pew Research Center, respondents were asked whether they would participate in a web-based system that their doctor's office used to manage patient records. Even in this scenario (which notably involved a much more transparent system than the one I'd used at the orthopedic surgeon's office), only a little more than half of American adults definitively said they'd be comfortable sharing their data.

Health data is one of the few categories of information that enjoy a robust (if outdated) set of privacy protections by law in the US, but the definition of what even counts as health data is rapidly evolving. More and more companies are looking to use diagnostic insights from social-media data and other nonregulated categories that currently exist in the lucrative marketplace of predictive analytics. The current Wild West environment allows health data brokers to create risk scores that are sold to insurance companies that in turn use these metrics to charge higher rates to the most vulnerable among us. Not only is this bad for patient privacy, but it further exacerbates inequalities in our society.

Care shouldn't require data consent

Americans' concerns about the sanctity of their health data have been cited as one reason that Google and Apple have recently partnered with the likes of the American Heart Association and doctors from Massachusetts General Hospital. Such household names can help allay patients' fears about entrusting their data to Big Tech. But we're now at the point where the stakes are growing much higher when we make decisions to share our data with a platform or participate in a study. When we opt in, we risk losing control over how our health data is used and who can profit from it. When we opt out, we risk losing access to the care we need.

In the era of data-driven medicine, systems for handling data need to avoid anything that feels like manipulation—whether it's subtle or overt. At a minimum, the process of obtaining consent should be separated from the process of obtaining care.

If you don't want to hand over your information right away, or if you have concerns about the security of your doctor's data-gathering efforts—you should be able to see the doctor anyway.

Mary Madden is a technology researcher and writer. She leads a project with the Data and Society Research Institute to understand the social and cultural impacts of data-driven technologies on health equity and well-being.