

With Consumer Privacy Center Stage, Why Aren't We Talking About Health Data?



By *Jamie Wells, M.D.* — May 30, 2018



Credit: Pixabay [1]

Protected personal health information has traditionally been exempt from privacy concerns, given the unique nature of its scope and regulation, until the advent of direct-to-consumer (DTC) genetic testing, forced implementation of electronic medical records (EMRs) and prescription drug monitoring programs. With such a recent public focus on Facebook's misleading policies over use of our data, [Europe's reactive efforts](#) [2] to govern the internet and the latest action to get the [California Consumer Privacy Act](#) [3] of 2018 on the [ballot](#) [4], it will be interesting to see what happens when the spotlight shifts to our protected health information that is currently flying under the radar.

As [NPR reports](#) [4], the California initiative, though not officially certified by the state, has garnered over 600,000 signatures which is twice as many required to qualify for November's ballot. If it passes, then the impact will be substantial to the state and yield potentially lasting effects for the country. According to [their website](#) [3], the measure's primary focus is



“Your personal information is being sold to businesses you don’t even know exist. The California Consumer Privacy Act will give you important new consumer privacy rights to take back control of your personal information. You have the right to tell a business not to share or sell your personal information. You have the right to know where and to whom your data is being sold or disclosed. You have the right to protections against businesses who do not uphold the value of your privacy.”

Why is this relevant to patient privacy

A keen insight into [their argument](#) [3] is the dependence on the internet as a tool to perform crucial life functions, like applying for a job. They make a compelling point about whether opting not to use it is a suitable alternative to curb data abuse and whether that is even feasible or reasonable today. This reality is not so distinct from the current state of digital use in the medical and healthcare sphere. Though distinctly protected under HIPAA laws, patient health information and access to it has entered murky territory. (1)

Examples of areas of concern in healthcare, starting with EMRs

When opting out of EMR use today is financially punitive and impossible given hospitals or health facilities dependence on them, where is the emphasis on patient-centered medicine? Review [here](#) [5] to appreciate how EMRs initially pitched as a long-sought concept of computerized universal personal health material that would mitigate issues with access and barriers to care never lived up to the hype and served to erode the doctor-patient relationship. In reality, when I speak of them, I am referring to what was actually delivered to physicians, billing platforms that marginalize meaningful patient data necessary to inform diagnosis and therapeutic interventions.

Under the guise of improving care, EMRs have served as a money grab for competing profit centers at the expense of physicians and patients (see [here](#) [5]). Their initial and continued mandated implementation also suggest they are in [violation of fundamental principles of bioethics](#) [5]. For example, with respect to basic tenets of autonomy, patients (and physicians) were never asked about the use of electronic medical records, how they would be rolled out and employed along with the ballooning access to protected health information they encourage. Patients were never fully instructed about the risks and benefits of the endless data these systems collect that often is not used at all to make treatment decisions on their care.

Prescription Drug Monitoring Programs

Consider the state of [prescription drug monitoring programs](#) [6] intended to centralize into a web-based data system prescription medications that met the criteria for [Schedule II-IV controlled substances](#) [7]. The goal was to provide a tool to identify and intervene when an individual might be developing signs of abuse, prevent doctor-shopping, ensure proper dosages and medication choices are made, side effects are well-managed and so on. Last summer, the [9th U.S. Circuit Court of Appeals reversed](#) [8] a 2014 U.S. District Court ruling that affirmed patients had a reasonable expectation of privacy with respect to their prescription records and mandated a court order be required before allowing federal agents the ability to obtain such data (see [here](#) [6]). With

this decision, the Drug Enforcement Administration (DEA) does not need to meet the standard of seeking a warrant based on probable cause and, instead, can routinely access such information.

That reversal was a bad day for the sanctity of the doctor-patient relationship, its therapeutic nature and the overall health —mental and physical— and well-being of patients. If a patient believes his health information is not protected, then he may not seek treatment and potentially further endanger himself and others depending on the etiology of the disorder or disease. Battles to preserve [patient's rights](#) [6] in this arena continue and may include a future visit to the U.S. Supreme Court.

Genome mapping

Look no further than last week's announcement by [Pennsylvania-based Geisinger Health System](#) [9] offering DNA sequencing to 1,000 patients as part of their primary care visit contending it should be included like any other routine testing. Absent among the [many talking points](#) [10] in their sales pitch of speculative claims at best (e.g. health care prevention of disease, possible reduction of healthcare costs) was any mention of the fact they are a health system and health insurance company (see [here](#) [10]). Is there a firewall between these functions for this data, or can it be used by actuaries to alter premiums and coverage? And while the data is stored within your health record who is the owner? Is Geisinger, like the direct-to-consumer companies, planning on licensing or selling genomic information?

In conclusion

The extent of this issue is rampant.

As new health-based technologies, innovative and not, continue to get a platform at warp speed, isn't it time we discern the difference first and be proactive in asking the right questions for the benefit of patients? This cycle of playing catch up after harm is done is outdated.

Notes

1. [Health Insurance Portability and Accountability Act \(HIPAA\) laws](#) [11] were instituted, in part, to secure the protection and confidential handling of health information with the most minimum-- in circumstances of third parties-- to be used to conduct business.

COPYRIGHT © 1978-2016 BY THE AMERICAN COUNCIL ON SCIENCE AND HEALTH

Source URL: <https://www.acsh.org/news/2018/05/30/consumer-privacy-center-stage-why-aren%E2%80%99t-we-talking-about-health-data-13033>

Links

[1] <https://pixabay.com/en/privacy-policy-data-security-445157/>

[2] <https://www.npr.org/sections/alltechconsidered/2018/05/24/613983268/a-cheat-sheet-on-europe-s-sweeping-privacy-law>

[3] <https://www.caprivacy.org/about>

[4] <https://www.npr.org/sections/alltechconsidered/2018/05/28/614419275/do-not-sell-my-personal-information-california-eyes-data-privacy-measure>

- [5] <https://www.acsh.org/news/2018/04/17/are-electronic-medical-records-ethical-12848>
- [6] <https://www.acsh.org/news/2017/08/23/big-brothers-latest-blow-patient-privacy-11724>
- [7] <http://www.deadiversion.usdoj.gov/schedules/>
- [8] <http://cdn.ca9.uscourts.gov/datastore/opinions/2017/06/26/14-35402.pdf>
- [9] <https://www.geisinger.org/about-geisinger/news-and-media/news-releases/2018/05/07/12/18/dna-sequencing-to-become-part-of-geisingers-routine-clinical-care>
- [10] <https://www.acsh.org/news/2018/05/25/precision-medicine-overselling-routine-dna-sequencing-primary-care-13014>
- [11] <http://www.dhcs.ca.gov/formsandpubs/laws/hipaa/Pages/1.00WhatIsHIPAA.aspx>