Editorial

Hospitals, Tech Giants, and Destruction of Patient Privacy

Lawrence R. Huntoon, M.D., Ph.D.

After the Health Insurance Portability and Accountability Act (HIPAA) of 1996 was passed into law and Congress failed to promulgate standards for the privacy and protection of individually identifiable health information, the Department of Health and Human Services was tasked with developing privacy standards.

In 1997, I traveled to Washington, D.C., and represented AAPS in providing comments to the National Committee on Vital and Health Statistics (an advisory committee to the HHS secretary) during the public comment period on the importance of patient privacy. In that day-long meeting we were informed that in the current environment, patients should have no reasonable expectation of privacy.

It was clear from the beginning that HIPAA was not designed to protect patient privacy. To the contrary, it allowed for a tremendous expansion of the number of people who would have access to the private information of patients. With the advent of electronic health records (EHRs), the destruction of patient privacy was enhanced and has become pervasive throughout the healthcare sector.

The Centrally Planned Debacle of Electronic Health Records

Electronic health records, which were supposed to reduce medical errors and improve quality of care, have done neither. EHRs were forced upon practicing physicians by the government-run Medicare program absent any meaningful input from the very people who would have to use them. A small sampling of brief excerpts from letters to the editor to the Wall Street Journal illustrates the problems that are well-known to physicians.[1]

> Electronic health record (EHR) systems are a clear and present danger and have vastly increased, not decreased, medical errors. In the past I could see 20 patients in a morning clinic. Now I see eight at most. However, because federal policies have forced me into employment by a hospital system and out of an independent private practice, I'm not the one losing money. [J. Joseph Perry, M.D.]
>
> EHRs were never developed by practicing physicians but were pushed on doctors, nurses and hospitals by central planners, Silicon Valley investors, software engineers and hardware manufacturers. Central planners and insurance companies wanted EHRs to manipulate physicians away from patients' needs in an attempt to bend the cost curve…. The American Recovery and Reinvestment Act of 2009 and the Affordable Care Act's funding for EHRs was pushed by lobbyists selling a false dream. [Howard C. Mandel, M.D.]
>
> Private doctors are usually reimbursed by set insurance-fee schedules without the ability to pass along increasing overhead costs to patients. The high cost of EHRs is a major reason many doctors become hospital employees. [Gerald J. Broock, M.D.]
>
> The doctors indicate that they spend hours of their workday as data-entry clerks. This only shows one side of the problem. The other is that so much data is generated, not even a speed reader could review the typical file. Too much information is as bad as no information. [Jay Tate]

New DNA Data Storage Advocated for EHRs

Indeed, the massive amount of digital data, in general, is growing at an overwhelming rate. International Data Corp has estimated that the world will produce about 160 zettabytes (one sextillion bytes) of data by 2025, more digital bytes than there are observable stars in the universe.[2]

As this is well beyond what current hard drives can handle, a new data storage technology has been developed—storing data in artificial DNA-encoded molecules. These DNA encoded molecules can, in turn, be embedded in nano-size silica glass spheres, which can store complete patient records in medical implants, prescription drugs, and virtually any other entity, including small plastic bunnies.[2] If you happen to lose an artificial DNA-encoded pill, eyeglasses, or plastic bunny, someone with the right equipment could decode and obtain your entire medical history.

Data Mining of EHRs Used to Avoid Clinical Trials

In an effort to cut costs and bring drugs to market more quickly, drug makers are using data from electronic health records to avoid having to perform clinical trials in patients. A law passed in 2016 "required the FDA to explore greater use of real-world data."[3] The data, however, may not be reliable as EHRs are often filled with inaccuracies and errors. This is to be expected since a priority of EHRs is to create a billing record to maximize payment by third-party payers. Hospitals hire coders who often engage in "creative coding," in order to maximize payments to the hospital. Creative coding may include listing disorders or diseases that are not actually diagnosed by physicians and documented by physicians in the medical record. This has unfortunately led to a situation in which the EHR may not be useful as an actual medical record. Instead of representing so-called "real-world data," it may

represent fantasy data that has little or no connection to the patient's actual medical condition.

Drug makers are eager to make more people eligible for the medications they produce and would likely be perfectly willing to use fantasy billing data in the EHR to gain FDA approval of their medications. The risk in using such unreliable data would include the FDA approving drugs that are not effective and may not be safe.

Project Nightingale

Meanwhile, Ascension, the nation's second-largest healthcare system, has struck a deal with Google to collect and analyze the detailed personal health information of millions of patients in 21 states.[4] This includes data from 2,600 hospitals, doctors' offices, and other facilities, including patient names, diagnoses, complete health history, and dates of birth.

Amazon, Apple, Microsoft, and the Mayo Clinic have struck similar deals with hospitals but nothing close to the magnitude or scope of Project Nightingale. Until the *Wall Street Journal* published its article on Project Nightingale, the project had essentially been kept secret from patients and their doctors. The *WSJ* article states, "…the Health Insurance Portability and Accountability Act of 1996, generally allows hospitals to share data with business partners without telling patients, as long as the information is used 'only to help the covered entity carry out its health care functions.'"[4] In addition, "at least 150 Google employees already have access to much of the data on tens of millions of patients."[4] The term "healthcare functions" can include virtually anything the hospital says it means.

Google is using the patient data to develop software combined with artificial intelligence hardware that "zeroes in on individual patients to suggest changes to their care."[4] Given the pervasive errors and inaccurate information in the electronic data set, garbage-in-garbage-out may have dire consequences for patients treated by the artificial intelligence computer.

Both Google and the Ascension system are looking to cash in on this new data-mining venture. Google hopes to sell similar lucrative products to other health systems, and Ascension "hopes to mine data to identify additional tests that could be necessary or other ways in which the system could generate more revenue from patients."[4]

Any new products developed by data-mining tech giants will also result in financial gain for hospitals based on agreements that include intellectual property rights.[5]

Patients who still value their privacy are essentially told they worry too much. According to the *WSJ* article, "Google co-founder, Larry Page, in a 2014 interview, suggested that patients worried about the privacy of their medical records were too cautious. Mr. Page said: 'We're not really thinking about the tremendous good that can come from people sharing information with the right people in the right ways.'"[4]

But, who are the "right people," and have they always been forthcoming in telling people what is going on? The *WSJ* article further states: "Last year, the Journal reported that Google opted not to disclose to users a flaw that exposed hundreds of thousands of birth dates, contact information and other personal data of subscribers in its now-defunct social-networking website Google Plus, in part because of fears that the incident could trigger regulatory scrutiny."[4]

In September 2019, Google agreed to pay $170 million in fines "and change its practices in response to complaints that it illegally collected data on children to sell ads."[4]

Also last September, Google and the Mayo Clinic entered a 10-year deal for Google to store the hospital system's "genetic, medical and financial records."[4] "Mayo officials said at the time that any data used to develop new software would be stripped of any information that could identify individual patients before it is shared with the tech giant," *WSJ* reported.[4]

However, two months later, *WSJ* published another article in which Mayo officials admitted that their deal with Google allows them to share personally identifiable information on patients, but they had no current plans to do so.[5] Whether current plans will change in the future, no one knows, but Mayo's chief information officer stated: "It was not our intention to mislead the public."[5]

Hospitals have become major brokers to tech companies in supplying patient data. Hospitals have struck deals with Microsoft, IBM, and Amazon, and "the breadth of access wasn't always spelled out by hospitals and tech giants when the deals were struck."[5] In a deal between Microsoft and Providence Health System, involving about 20 million patient visits per year, doctors' "notes haven't been stripped of personally identifiable information, according to Providence, which is based in Renton, Wash."[5] According to Providence's chief information officer, "executives involved in the agreement at first planned to use data without information identifying patients; later they found they couldn't remove it all from doctors' notes. 'It was not intended to mislead,' he said."[5]

There seems to be a developing pattern in which those entering into these privacy-destroying alliances between hospitals and tech giants assure the public that their private information will not be shared, but then when inquiring journalists discover that private confidential medical information is being shared, the response is that there was no intent to mislead the public.

The Centers for Medicare and Medicaid Services (CMS) make it clear that patients do not own their own private medical information. Medical privacy is a myth. "'Hospitals are massive containers of patient data,' said Lisa Bari, a consultant and former health information technology lead for the CMS Innovation Center. Hospitals can share patient data as long as they follow federal privacy laws, which contain limited consumer protections, she said. 'The data belongs to whoever has it.'"[5]

WSJ went on to report: "'The patient doesn't have absolute control. They don't have much control,' said Ellen Wright Clayton, a Vanderbilt University biomedical ethics professor. Under HIPAA, hospitals must divulge as little as possible about patients under agreements. But in some cases, the minimum amount needed by tech companies can be everything in patients' records."[5] The data can include names and Social Security numbers, and the hospitals are not required to

notify patients of specific data shared with tech companies. According to Ascension's chief strategy and innovations officer, "By definition this means that the 'minimum' necessary dataset for the creating of this capability is the entire longitudinal health-care record for each patient."[5]

Conclusion

A patient's personally identifiable medical information is no longer private, as a result of HIPAA and the federal government's actions to force hospitals and physicians to adopt EHRs. Hospitals have sent patient names, birth dates, Social Security numbers, diagnoses, medications, surgical histories, and genetic and medical histories to tech giants, which use the data to financially benefit both the tech companies and the hospitals. Patient consent for the sharing of their personal information with tech giants and others is not required by HIPAA, and the only way patients can maintain their privacy is to see physicians who are not in the third-party-payment system. Physicians who are opted out of Medicare and who have no contracts with any insurance companies do not file claims and do not violate the Oath of Hippocrates by sending the patient's private information to tech giants and others. What a sad state of affairs when dogs, cats, and other pets have more medical privacy than humans.

Lawrence R. Huntoon, M.D., Ph.D., is a practicing neurologist and editor-in-chief of the *Journal of American Physicians and Surgeons*. Contact: editor@jpands.org.

REFERENCES

1. Letters. Doctors debate electronic health records, *WSJ*, Apr 9, 2018. Available at: https://www.wsj.com/articles/doctors-debate-electronic-health-records-1523277236. Accessed Feb 9, 2020.
2. Hotz RL. This toy stores data in DNA. *WSJ*, Dec 10, 2019. Available at: https://www.wsj.com/articles/scientists-store-data-in-synthetic-dna-embedded-in-a-plastic-bunny-11575907200. Accessed Feb 9, 2020.
3. Loftus P. Drugmakers mine data to avoid clinical trials. *WSJ*, Dec 23, 2019. Available at: https://www.wsj.com/articles/drugmakers-turn-to-data-mining-to-avoid-expensive-lengthy-drug-trials-11577097000. Accessed Feb 9, 2020.
4. Copeland R. Google's 'Project Nightingale' gathers personal health data on millions of Americans. *WSJ*, Nov 11, 2019. Available at: https://www.wsj.com/articles/google-s-secret-project-nightingale-gathers-personal-health-data-on-millions-of-americans-11573496790. Accessed Feb 9, 2020.
5. Evans M. Hospitals give tech giants access to detailed medical records. *WSJ*, Jan 20, 2020. Available at: https://www.wsj.com/articles/hospitals-give-tech-giants-access-to-detailed-medical-records-11579516200. Accessed Feb 9, 2020.