The Illusion of Patient Privacy and Private Practice

Susan Israel, M.D.

While studying history in high school, I laughed at the 19th-century Luddites for fearing the mechanization of manufacturing. Now I feel like one of them for fearing the mechanization of medical records that makes patient privacy almost impossible.

I never dreamed our rights to privacy would be so overridden by the taking of our electronic medical records and insurance claims data for oversight and research without consent, particularly as the research may not be nuanced enough to successfully guide an individual patient's treatment plan, but will be used by governments and insurers to direct patient care and control the practice of medicine.

This control is achieved by using research to create treatment "guidelines" that will be used to define "quality care" that physicians will be pressured to follow in order to be "paid for performance." Or, the research will be used to justify mandating which treatments will or will not be paid for. If "cost effectiveness" is a criterion used in the research, a chemotherapy drug might be denied for not saving enough lives, or an aortic valve replacement denied because the patient is supposedly too old to justify its cost. This would become de facto rationing of care tucked into the mandated treatment guidelines.

The federal Department of Health and Human Services (HHS) is financing development of "medical homes" to deliver patient care through State Innovation Model (SIM) bureaucracies.¹ These will be in the forefront, along with Medicare, Meaningful Use, and Medicaid, in implementing the "pay for performance," "quality care" and "scorecard" reimbursement scales for physicians, creating a de facto single-payer system. This will be accomplished through collaboration of health plans with state and federal governments.² Patient and physician behavior will be tracked, scrutinized, studied, and used for research, using the electronic medical record and insurance claims data. This effectively will eliminate the privacy of medical practice and remove it from the rest of the U.S. free-enterprise economic system. Lack of competition and choice in the medical system will degrade it. Physician initiative will decline, and patients will have no recourse but to accept the treatments mandated for them by the monolithic, government-controlled system.

In 2002, HHS modified HIPAA's "Privacy Rule"³ to eliminate patient consent for identified data being seen for treatment, payment, and healthcare operations (a 390-word definition including quality control, tech support, business

associates, covered entities, etc.).⁴ Additionally, HIPAA provisions⁵ allow federal and state oversight agencies, including HHS, researchers, and healthcare clearinghouses to see records without patients' consent.⁶ The breadth of identified medical data (including hospital discharge data) going to public health departments is jaw-dropping, and now is more at risk as it is sent over the Internet. Thus, regardless of audit trails and passwords, the confidentiality of patient data depends on hundreds of people in clinics, hospitals, corporations, and government agencies nationwide not leaking or misusing it. Unfortunately, the electronic record makes intimate information more readily available to many more people who could use it to bias an individual's application for employment, schools, or the military, or worse, use it to exert political pressure on a government official or legislator.^{7,8,9} Further, as we know, hackers are busy accessing the medical data of millions of people for profit and electronic espionage.¹⁰

A national Health Information Exchange (HIE) is planned for electronic health records, giving its access to medical practitioners across the country and to government oversight agencies.¹¹ Unless the HIPAA rule is rescinded or patient consent restored, we will not be able to control who sees our records even if we are given the details of any security provisions. When the public becomes aware of the broad access to their private records, many will not disclose needed medical history until their illnesses are so advanced it costs the system even more for treatment. For psychiatric patients refusing to seek treatment, one would expect increases in suicide and homicide.

Additionally, our health insurance claims data are being released to researchers and government agencies by the All-Payer Claims Databases (APCDs). These have been created by 14 states (with five states in implementation, including Connecticut and New York)¹² to mandate that the health plans turn over medical and pharmacy claims data, including all diagnoses, procedures, tests, drugs prescribed, providers' names with dates and identifiers (which can include enrollment data and Social Security numbers), all to a massive database managed by the state or a private company under state contract. These data are then sent to researchers in identified or de-identified forms, with varying degrees of privacy protections that attempt to prevent re-identification and leaks.

On one end of the APCD spectrum is Colorado, which may release identified claims data under extremely rare circumstances to state-approved research or public health

entities. The Application to the APCD Administrator to Approve the Release and Use of Colorado All Payer Claims Data states that "this application is for a limited data set or identifiable information." This is available at the CIVHC/ CO APCD Data Release site,13 by clicking on "Data Release Pre-Application." But Colorado and other states accept only a signature as proof that the data have been destroyed after use, in spite of the existence of a large market for the purchase of medical information. On the other end is Rhode Island,¹⁴ which allows its citizens to opt out of the APCD and does not take their names and addresses. However, to know whether the data still could be reidentified by managers and researchers, one would need to know the exact details of the data used and its handling. Massachusetts¹⁵ is another example of a developed APCD with a comprehensive patient data submission guide for insurers.

States such as Oregon¹⁶ can release "limited data sets"^{17,18} to researchers,⁴ which are still considered identified and protected health information (PHI), because only 16 of the 18 HIPAA identifiers have been taken out, leaving the full date of birth (month, day, year) and the full ZIP code with the gender and other medical data. However, it has been shown that 63–87 percent of the population can be identified by merging those demographics alone (birth date, ZIP code, and gender) with other data bases such as voter registration lists.^{5,6,19,20,21}

As noted earlier, identified medical information can be released for the purposes of the APCDs, public health, researchers, government oversight agencies, healthcare operations, etc., without patient consent. But even with the 18 identifiers removed as specified by HIPAA for deidentification (Safe Harbor method), it is no longer as private as it might have been 15 years ago, before the explosion of online databases. Thus the re-identification rate for this supposedly de-identified data is not zero.

By using solely the demographics of HIPAA deidentified data, the re-identification rate of patients has been shown to be 0.04% (using the year of birth, threedigit ZIP Code for populations greater than 20,000 and gender) to 0.22%, (using the year of birth, three-digit ZIP, marital status, ethnicity, and gender), that is up to 2,200 people per million, according to Latanya Sweeney, Ph.D., of Harvard,²² and Deborah Lafky of HHS,²³ respectively. However, those re-identification rates would be much higher if the accompanying medical histories were added to the demographics when merged with the other online databases. It is also important to note that once medical records are released in the HIPAA de-identified form, they are no longer considered protected health information (PHI) and protected by the HIPAA privacy rules, even if they subsequently could be re-identified as described above.

In the short term at least, the APCDs are raising medical costs as the third-party payers raise premiums to cover

their costs of sending data to the APCDs, and researchers often must buy our data to finance the APCDs. Colorado, for example, advertises prices of \$25,000 to \$150,000 for the purchase of de-identified data and limited data sets (see "Pricing & Funding" under the "Get More Data" tab).24 The result of these APCDs is the creation of a lifetime (for a newborn) medical dossier on all of us, which we can only hope is not hacked, misused, or re-identified when distributed. Whether or not the states can force the selfinsured health plans to turn over patient health insurance claims data to their All Payer Claims Databases is now being heard before the U.S. Supreme Court in Gobeille v Liberty Mutual Insurance Company. Hopefully, the Supreme Court will consider patient privacy rights along with interpreting the ERISA status of the self-insured plans that may allow them not to comply with participating in the state APCDs.

These APCDs, health insurance exchanges, and the medical homes are costing billions of dollars that the federal and state governments have taken from direct patient care and medical practitioners and given to their non-medical professional bureaucrats in the hope that they can improve medical care!

At the very least, all electronic medical systems must be structured with consent requirements so that patients can control who sees their records, as was done in the "old days" when paper records, doctors' handwriting and metal cabinets protected them. Paper medical records can be shredded after seven years or so, depending on each state's law,²⁵ but now with the electronic medical record, it will be easier for the records to remain permanently recorded and available.

There are developed technologies for patients to keep some information from the rest of the record (segmentation, for example) and to alert a physician that information has been left out. Both should be installed into the electronic systems regardless of cost and complexities involved. As physicians, we need to advocate for record systems that engender trust and enable us to fulfill our Hippocratic Oath to protect patient information from further disclosure.

One breakthrough for privacy recently occurred when the U.S. Court of Appeals for the 2nd Circuit ruled that NSA's taking of everyone's phone records is not allowed by the USA PATRIOT Act. Most importantly, the ruling raises "one of the most difficult issues in Fourth Amendment jurisprudence: the extent to which modern technology alters our traditional expectations of privacy." Also, the Court stated, "If the government is correct, it could use [the law] to collect and store in bulk any other existing metadata available anywhere in the private sector, including metadata associated with financial records, medical records...."

I hope this ruling can be used by physicians to bolster our efforts to ensure and protect patient privacy and to convince governments, insurers, hospitals, researchers, and technology companies of this necessity. We need to foster a public debate over citizens' right to medical privacy vs. government seizure of private information without consent, because any loss of privacy rights undermines our society, and threatens our freedoms and our way of life.

Susan Israel, M.D., is a psychiatrist and patient privacy advocate in Connecticut. Contact: sisrael78@optonline.net.

REFERENCES

- Centers for Medicare and Medicaid Services. State Innovation Models Initiative: General Information; Oct 5, 2015. Available at: www.innovation. cms.gov/initiatives/state-innovations/. Accessed Nov 2, 2015.
- Office of Health Reform and Innovation. Connecticut State Innovation Model Test Grant Application. Available at: www.plan4children.org/wp-content/ uploads/2014/08/Project_Abstract_-_Final.pdf. Accessed Nov 2, 2015.
- 3. Patient Privacy Rights. The Truth about HIPAA; 2015. Available at: www. patientprivacyrights.org/truth-hipaa/. Accessed May 6, 2015.
- Citizens' Council for Health Freedom (formerly Citizens' Council on Health Care). HIPAA Definitions: Treatment, Payment and Health Care Operations; April 2005. Available at: www.cchfreedom.org/custom/?keywords=HIPAA+d efinitions#.Va4tpVLbL1c. Accessed Jul 21, 2015.
- Office of the National Coordinator for Health Information Technology. Guide to Privacy and Security; April 2015. Available at: www.healthit.gov/sites/ default/files/pdf/privacy/privacy-and-security-guide.pdf. Accessed Apr 22, 2015.
- U.S. Department of Health and Human Services, National Institutes of Health. How Can Covered Entities Use and Disclose Protected Health Information for Research and Comply with the Privacy Rule? Available at: https:// privacyruleandresearch.nih.gov/pr_08.asp. Accessed Nov 2, 2015.
- Patient Privacy Rights. Learn about Health Privacy; 2015. Available at: https:// patientprivacyrights.org/learn-about-health-privacy/. Accessed Jul 22, 2015.
- Anderson N. "Anonymized" data really isn't—and here's why not. Law & Disorder/Civilization & Discontents. Ars Technica; Sep 8, 2009. Available at: www.arstechnica.com/tech-policy/2009/09/your-secrets-live-online-indatabases-of-ruin/. Accessed Nov 3, 2015.
- Defense Advanced Research Projects Agency. DARPA "Brandeis" program aims to ensure online privacy through technology. Press Release, Mar 11, 2015. Available at: http://www.darpa.mil/news-events/2015-03-11. Accessed May 6, 2015.
- Sternstein A. Blackmail lists? Bribery? Why background check files keep getting hacked. Nextgov.com, Apr 28, 2015. Available at: http://m.nextgov. com/cybersecurity/2015/04/why-federal-employee-background-checkfiles-keep-getting-hacked/111355/. Accessed Nov 3, 2015.
- HealthIT.gov. Health Information Exchange (HIE) What is HIE? Available at: www.healthit.gov/providers-professionals/health-information-exchange/ what-hie. Accessed May 5, 2015.

- 12. All-Payer Claims Database Council. Interactive State Report Map. Available at: www.apcdcouncil.org/state/map. Accessed Nov 3, 2015.
- Center for Improving Value in Healthcare. Pre-application request for Colorado APCD data. Available at: http://civhc.org/All-Payer-Claims-Database/Data-Release-Review-Committee.aspx/. Accessed Nov 9, 2015.
- 14. Rhode Island Department of Health. All-Payer Claims Data Base Project. Available at: www.health.ri.gov/partners/collaboratives/ allpayerclaimsdatabase/. Accessed Apr 16, 2015.
- Center for Health Information and Analysis, Massachusetts All Payer Claims Database. All Payer Claims Database Data Submission Guides, Version 4.0. Available at: www.chiamass.gov/apcd-data-submission-guides. Accessed Apr 15, 2015.
- Oregon Health Authority, Office of Health Analytics, All Payer Claims Data Reporting Program. Form APAC-5: Research Application for Limited Data Sets. Available at: www.oregon.gov/oha/OHPR/RSCH/docs/All_Payer_all_ Claims/APACS_v2015_1.4.3.15.pdf. Accessed Apr 15, 2015.
- U.S. Department of Health and Human Services, National Institutes of Health. Health Services Research and the HIPAA Privacy Rule; May 20, 2005. Available at: http://privacyruleandresearch.nih.gov/healthservicesprivacy. asp. Accessed Jun 10, 2015.
- Office of Human Subjects Research—Institutional Review Boards. Definition of limited data set. *Johns Hopkins Medicine*; April 2015. Available at: www. hopkinsmedicine.org/institutional_review_board/hipaa_research/limited_ data_set.html. Accessed Jun 10, 2015.
- Sweeney L. Simple demographics often identify people uniquely. Carnegie Melon University Data Privacy Working Paper 3; 2000. Available at: http:// dataprivacylab.org/projects/identifiability/paper1.pdf. Accessed Nov 3, 2015.
- TheDataMAP. Matching known patients to health records in Washington State data; 2012-2013. Available at: www.thedatamap.org/risks.html. Accessed Nov 3, 2015.
- 21. TheDataMap. All the places your data may go; 2012-2013. Available at: www. thedatamap.org/. Accessed May 4, 2015.
- 22 National Committee on Vital and Health Statistics Ad Hoc Work Groups for Secondary Uses of Health Data. Hearing Proceedings; Aug 23, 2007. Available at: www.ncvhs.hhs.gov/transcripts-minutes/transcript-of-the-august-2-2007-ad-hoc-workgroup-for-secondary-uses-of-health-data-hearing/. Accessed Nov 3, 2015.
- Kwok P, Davern N, Hair EC, Lafky D. Harder than you think: a case study of re-identification risk of HIPAA-compliant records. Abstract. Joint Statistical Meetings, Miami Beach, Fla., 2011. Available at: www.amstat.org/meetings/ jsm/2011/onlineprogram/AbstractDetails.cfm?abstractid=302255. Accessed Nov 3, 2015.
- 24. Center for Improving Value in Healthcare. Application to the APCD Administrator to Approve the Release and Use of Colorado All Payer Claims Data. Available at:www.comedprice.org/. Accessed Nov 3, 2015.
- 25. Healthit.gov. State medical records laws: minimum medical record retention periods for records held by medical doctors and hospitals. Available at: www. healthit.gov/sites/default/files/appa7-1.pdf. Accessed Nov 3, 2015.