Electronic Health Records: Balancing Progress and Privacy

Ross White, 06/19/2012

Regardless of the fate of the Affordable Care Act, it has set in motion a drive toward greater use of information technology, particularly with regard to electronic health records (EHRs). These technologies promise to increase the transmission, sharing, and use of health data across the health care system, thereby improving quality and reducing unnecessary costs. But they do not come without raising serious ethical questions, particularly those related to privacy. This was the topic of the 2nd International Summit on the Future of Health Privacy hosted by Patient Privacy Rights at Georgetown Law School on June 6 and 7. The two-day event brought together national and international experts on health privacy, technology, and law; patient advocates; industry experts; and top governmental officials to discuss whether there is an American health privacy crisis.

The incentives to implement electronic health record systems have never been greater. The Health Information Technology for Economic and Clinical Health Act (HITECH Act), which is a portion of the American Recovery and Reinvestment Act of 2008 (ARRA), designated incentive payments of up to $44,000 from Medicare and $65,000 from Medicaid per individual physician who demonstrate meaningful use of an EHR system. Providers who do not demonstrate meaningful use of EHRs by 2015 will be penalized with a 1 percent annual reduction in Medicare reimbursements. While many physicians are embracing this opportunity, others continue to resist or have already experienced adverse effects after having done so.

One anecdote from the Summit perhaps best captures what is at stake. Scott Monteith, clinical assistant professor in the Departments of Psychiatry and Family Medicine at Michigan State University, relayed the story of a patient who found that her electronic medical record erroneously indicated a history of inhalant abuse. After much investigation and confusion, it was revealed that the patient actually had a history of caffeine dependence and intoxication (yes, this is a real diagnosis), which shares the same diagnostic code (305.9) as inhalant abuse. Although this diagnostic code is used for four different diagnoses, the default EHR window only made the inhalant abuse diagnosis visible to the physician. Despite reporting the error to the EHR vendor, the problem persists.

In addition to errors, the Summit also raised concerns that data in digital form is far easier than paper data to be obtained illegally or used against the patient's wishes. Mark Rothstein, Herbert F. Boehl Chair of Law and Medicine at University of Louisville School of Medicine, emphasized that context is a critical consideration for health privacy protection. There are over 25 million "compelled authorizations" per year--a term Rothstein uses to refer to the legal acquisition of an individual's health records by employers, insurers, the criminal justice system, and other parties as a condition of applying for or obtaining employment, insurance, or public benefits. Rarely does an individual's entire health record need to be transmitted to the requesting party, yet the default is to do so, putting extraneous health data in many people's hands. An employer who needs to assess whether an employee is physically fit to perform a job has no business knowing that the employee had a bout of depression when he was a teenager or has a genetic propensity to develop Alzheimer's disease. The flood of information now available and transmitted by electronic health records has the potential to lead to unprecedented levels of discrimination.
While there have been efforts to prevent health discrimination of some sorts, such as the Genetic Information Nondiscrimation Act of 2008 (GINA), they are limited in their scope. GINA, for instance, addresses genetic discrimination for employment and health insurance, but offers no such protections for life insurance or long-term care insurance.

Many participants at the meeting anticipated that the use, and misuse, of individual genetic information will only accelerate in the coming years as clinicians encourage their patients to have their whole genome sequences, which some claim will cost less than $1,000 by the end of this year. Laura Rodriguez from the National Human Genome

Research Institute of the National Institutes of Health emphasized that genetic information has much greater levels of complexity and understanding than other health data; is uniquely identifiable to a single patient; has familial implications; can impact individual reproductive decision-making; and can have broader community and cultural meaning. For these reasons, it appears the protection of genetic information will not only be more important than other health data, but also more challenging as our understanding of the genome continues to evolve.

Whether dealing with genetic or nongenetic information, perhaps the most interesting thing to come out of the Summit was a proposed Consumer Health Privacy Bill of Rights. Modeled on the Consumer Privacy Bill of Rights released by the White House in February (which did not include specific protections for health information), the draft makes a forceful case for increased protections by Congress, stating that more than 40 million Americans have had the privacy of their electronic health records breached in the past 15 years. It proposes 10 principles, starting with the right to individual control – that consumers have a right to exercise control over what personal health information is collected about them and how it is used, including the right to limit disclosure of specific and sensitive information.

No doubt I agree with these basic guiding principles, but formal legislative adoption and implementation appears highly unlikely. Financial interests of health IT developers, the health care industry, and providers will likely make it difficult to resist the inertia in the health care system toward the belief that more information is always better and the need to stay at the forefront of innovation. The further deployment of health IT and EHRs is wholly consistent with increasing pressure on providers and insurers to try to improve the quality and decrease the cost of health care through delivery and payment reforms.

But innovation can come at the cost of patient privacy, autonomy, and respect, and technology is not a panacea for all that ails the health care system. As Mark Rothstein emphasized, HIPAA and other privacy regulations have unfortunately become the ceiling, rather than the floor for health privacy. Patients must insist that health privacy protections continue to expand with new technologies, not continue to simply meet the bare minimum.
Many difficult questions remain about ensuring adequate health privacy. How should we adequately balance the promises of quality improvement and clinical effectiveness made possible with EHRs against the right of patients to know how and when their health information is being used? Who owns health data: the patient or the providers who record it? Where should this data be stored: at the office of the health provider or in the "cloud" behind a secure network?

Based on failed attempts at health privacy and medical record sharing in Europe, Ross Anderson, professor of security engineering at Cambridge University, argued that data should be kept at the provider, not in large central databases vulnerable to attack. He also insisted that patients be notified every time their health information is shared with another provider for secondary use and that we must be willing to draw "red lines" that should not be crossed with health data use.

Most importantly, Anderson argued that our health privacy system should move from one of consent law to veto law. Rather than patients having the right to consent to the use of their health data, they would instead have the right to veto the use of their health data. Although this may appear to simply be a matter of language and messaging, it might better empower patients to know that they have a right to say "no," not just a right to say "yes." This is but one step in reconfiguring how our health care system ensures the protection of health privacy, but this progress may well be the beginning of a deeper examination of how we can more meaningfully balance technological progress with patients' rights.

Ross White is the public policy associate at The Hastings Center and a graduate student in philosophy and social policy at George Washington University. Follow him on Twitter @rossswhite.