

# BIOETHICS FORUM

DIVERSE COMMENTARY ON ISSUES IN BIOETHICS

## Debate Over Patient Privacy Control in Electronic Health Records

**Mark A. Rothstein**

Posted 02/17/2011

The percentage of physicians using an electronic health record (EHR) system has increased substantially in the last year, with encouragement from Medicare and Medicaid incentives included in the American Recovery and Reinvestment Act of 2009. Half of all office-based physicians use some form of EHR, according to a survey in December by the Centers for Disease Control and Prevention, although only 10 percent have fully functional EHR systems.

EHRs hold great promise for more effective and efficient health care. When fully implemented, they will be interoperable, allowing disparate systems and networks to send and receive information across the country. They will be longitudinal, including all of an individual's health care encounters over extended periods of time. They also will be comprehensive, containing the records of all visits with physicians and other health care providers, such as dentists, chiropractors, and physical therapists.

The same qualities that make EHRs valuable also raise serious privacy concerns. Unlike information in fragmented paper records, electronic information can be easily located and accessed. Thus, old, sensitive information with no current clinical utility will never go away; it will remain in an individual's health records indefinitely.

At public hearings in Washington on February 15 and 16, two advisory committees of the Department of Health and Human Services heard from five panels of experts and stakeholders on options for addressing privacy concerns raised by EHRs.

Among the top privacy concerns is that a wide range of health care providers will have access to information that they do not need to know. For example, a dentist filling a cavity ordinarily does not need to see an individual's reproductive health history.

Second, individuals applying for a job or insurance (e.g., health, life, disability, long-term care) are often required to sign an authorization disclosing their health records, and typically this involves complete records. There are at least 25 million such disclosures each year, and third-party access to comprehensive EHRs could lead to embarrassment, stigma, and discrimination.

Third, many patients already engage in "defensive" practices with their physicians to limit the amount of sensitive information in their health records, even though doing so could interfere with optimum health care. The use of these practices will likely increase unless privacy controls are available in EHRs. Public health and safety could also suffer if individuals with stigmatizing conditions, such as sexually

transmitted infections, substance abuse, and mental health problems, avoid prompt treatment because they fear the information will be a permanent part of their records.

There are three main approaches to privacy in EHRs. First, many physicians assert that patients should not be able to control the content of their health records because doing so would fundamentally change medical practice. This argument overestimates the utility of current records and underestimates the decrease in health privacy that would take place if EHRs were adopted without any patient privacy controls. It is highly unlikely this position will prevail.

Other experts say that patients should be able to control the content of their health records down to the individual data element. In December, the President's Council of Advisors on Science and Technology issued a series of recommendations, including using "tagged data elements." This approach, which has not been used with health records, would permit highly granular aggregation of data elements for treatment, quality assurance, public health, and research uses. It would also enable patient-selected privacy controls to be "tagged" to data wherever it travels, thereby aligning disclosures with patient instructions. Under such an approach, individuals would have "item-by-item" control over access to their health information.

At first blush, this proposal would seem to promote patient privacy interests, but even if it were technically feasible it would be totally impractical. Patients would need to review all of their health records and select specific items they wanted to tag with privacy controls. This process would be time consuming and burdensome for patients and providers, and it would require extensive staff training, patient education, and technical support.

In April 2003, when the Health Insurance Portability and Accountability Act (HIPAA) privacy rule went into effect, there was widespread confusion, frustration, and uncertainty among providers and patients, even though HIPAA's notice of privacy practices and patient acknowledgement of them are relatively simple. The complexity of data tagging choices and procedures might cause many patients to opt out of health information exchange or waive all of their privacy rights.

Besides logistical concerns, granular and unlimited patient privacy controls could severely disrupt patient care and therefore would be strenuously opposed by physicians and other providers. In effect, EHRs would be converted into personal health records; patients could deny access to any item of health information, and providers would not necessarily know the item even existed. Thus, a patient on a liver transplant list could tag the reference in his or her record indicating the patient was continuing to consume six beers per day. EHRs should not give rise to a cat-and-mouse game of providers adding and patients "tagging" sensitive information.

The National Committee on Vital and Health Statistics (NCVHS), a federal advisory committee to the Secretary of Health and Human Services, has proposed a middle ground between no patient privacy controls and granular controls. Based on extensive public hearings between 2006 and 2010, the NCVHS recommended that patients have the option of sequestering sensitive health information in one or more predetermined categories, such as reproductive health, mental health, substance

abuse, domestic violence, and genetic information. These categories and their contents would be known by patients and providers.

The NCVHS proposal would be easier for patients because they need not review their entire record, but could simply indicate that they wanted to sequester, for example, their mental health information from disclosure without additional consent. The proposal also would be less objectionable to providers, because only certain categories of information could be sequestered, and providers would know when they needed to obtain additional information from the patient or access to sequestered information. Segmented privacy controls could be used with a granular data element approach to health information exchange, but there have been no explicit proposals to do so.

Patient privacy controls will be an essential part of the electronic health records being developed in the private sector and coordinated by the Department of Health and Human Services. In considering what privacy controls to adopt, it is imperative that policy drive technology, not the other way around. Patient privacy controls based on sound policy should: (1) have low initial and recurring costs; (2) be easy to understand by patients and providers; (3) not require excessive time or effort in making choices; (4) not cause a lot of patients to opt out of health information exchange or avoid selecting any privacy controls; (5) not impose excessive administrative burdens on providers; and (6) not unnecessarily interfere with clinical care. These principles should drive HHS's decision in selecting patient privacy controls.

Mark A. Rothstein, JD, is the Herbert F. Boehl Chair of Law and Medicine and Director of the Institute for Bioethics, Health Policy and Law at the University of Louisville School of Medicine. From 1999 to 2008 he was a member of the NCVHS, where he chaired the Subcommittee on Privacy and Confidentiality. He currently serves as a member of the PCAST Report Workgroup of the HIT Policy Committee, which reports to the Office of the National Coordinator of Health Information Technology at HHS. The views expressed here are solely the author's.