THE NATIONAL LAW JOURNAL

JUNE 8, 2009

Daily Updates at NLJ.COM

Electronic records mandates may clash with privacy laws

Patchwork of state laws adds complexity.

BY ERIC A. KLEIN AND CHRISTINE C. COHN

President Obama has declared that electronic medical records will "reduce error rates, reduce our long-term cost of health care and create jobs." "Obama's Prime Time Press Briefing," N.Y. Times, Feb. 9, 2009. Congress has authorized $19 billion to implement provisions of the American Reinvestment and Recovery Act of 2009 intended to accelerate the adoption and use of "certified electronic health record [EHR] technology" during the next several years by hospitals and physicians that provide services to Medicare and Medicaid beneficiaries. H.R. 1, 111th Cong. §§ 4001-4201 (2009). Professionals and hospitals that fail to implement EHR technology by 2014 stand to suffer reductions in Medicare reimbursements.

The goal of this campaign is to adopt EHR technology to replace the current paper and fragmented computer files maintained by the vast majority of hospitals and physicians. Imagine a health information technology (HIT) system that includes all of a patient's diagnoses, medical history, laboratory and test results, medications prescribed, payor claims data, hospital records and other pertinent data. That system would be available to a patient's health plan, hospital, pharmacy and doctors. Payors and regulators also can use this type of system to reduce fraud, waste and duplication, as well as control processing costs and improve disease-state management programs. EHR technology promises to reduce medication and other medical errors and streamline clinical decision-making and communication.

That "holy grail" has been envisioned by many participants in the health care industry today, but unfortunately it is not achievable under the current patchwork of federal and state laws and most existing HIT systems. In its ambitious effort to hasten the advent of EHR for the 21st century, the federal government actually may be working at cross-purposes with privacy protections established under federal and state law. Here's why.

CONFIDENTIALITY MANDATES

First, existing law mandates the daunting task of obtaining individual patient consents. Health information of a particularly sensitive nature, such as records concerning an individual's treatment for mental illness, drug addiction or alcohol abuse, creates uniquely complicated legal and practical problems with respect to interoperable EHR technology. For example, federal law protects the confidentiality of records regarding the identity, diagnosis and treatment of any patient if such records are maintained in connection with an alcohol or drug abuse treatment program that is regulated or directly or indirectly assisted by a federal program. 42 U.S.C. 290dd-2. With few exceptions, such health records cannot be disclosed, even among health care providers for purposes concerning medical treatment, without the patient's prior written consent. § 290dd-2(b).

Consequently, absent a patient's prior authorization, clinical laboratory test results produced by a federally funded hospital program that indicate or reveal the patient's treatment for drug addiction apparently have to be segregated or omitted from any other information entered by the hospital in the patient's EHR, or otherwise shielded from disclosure to other health care providers. Of course, the issue of segregating and omitting such information from the patient's health record predated the advent of EHR, but it is precisely the integrated and cumulative nature of EHR that necessitates additional security and privacy measures to prevent the unauthorized disclosure of sensitive health records.

The patchwork of state laws protecting the confidentiality of sensitive health data adds another layer of complexity to a broad adoption of EHR technology. Statutory safeguards against the unauthorized disclosure of HIV test results illustrate this problem. Let's compare California and New Mexico. In California, a health care provider who negligently discloses an individual's HIV test results to a third party in a manner that identifies or provides identifying characteristics about the individual may be liable for civil penalties and damages. Calif. Health & Safety Code § 120908. New Mexico bars any person who administers an HIV test from disclosing the test results to another health care provider without the prior written consent of the tested individual or the individual's legally authorized representative, if the disclosure is made in a manner that permits identification of the tested individual and the health care provider to whom the disclosure is made does not have a "need to know such information." N.M. Stat. Ann. § 24-2B-6. So a disclosure of the HIV test results contained in the same cyberspace record could be barred in California but permitted in New Mexico.

The HITECH ACT, which passed as a component of the economic stimulus legislation, significantly expands security and privacy protections.

To make things even more interesting, New Mexico recently enacted its own Electronic Medical Records Act. N.M. S.B. 278. One provision of the new law requires a health care provider who requests information in an EHR using a record-locator service or health-information exchange to warrant that the request is for the treatment of the individual, is permitted by the individual's written authorization or is otherwise permitted by state or federal law.

Health plans are certain to face compliance issues of no less difficulty than those confronting providers. For example, if a health plan wishes to provide its contracting health providers in several states with access to an interoperable EHR system containing clinical laboratory test results for the plan's members, the disclosure of such information through the interoperable system is bound to miss the mark under a given state's particular configuration of confidentiality safeguards.

What solutions might be available? Obtaining patient authorization for every release of information through interoperable EHR is plainly unrealistic and self-defeating from the perspective of the efficient and timely exchange of information. One possibility is to mandate electronic firewalls that shield sensitive information regarding diagnoses and treatment for mental illness, alcoholism, drug addiction and sexually transmitted diseases. Current HIT systems have not contemplated such segregation or shielding of information and may not be easily modified to fit such requirements. Another obvious problem is the firewall's implicit disclosure of the mere fact that at least one of these items exists in the record.

An alternative might be federal legislation that would pre-empt state law and immunize providers for disclosures made via an EHR—if such disclosures were made in good faith and for purposes of health care treatment or other specified legitimate purposes.

FEDERAL PRIVACY RESTRICTIONS

The sweeping Health Insurance Portability and Accountability Act of 1996, 42 U.S.C. 1320d-1320d-8 (HIPAA), generally requires health care providers, health plans and other "covered entities" to make reasonable efforts to limit the protected health information that they request, use or disclose regarding an individual to only the minimum such information necessary to accomplish the intended purpose of the use, disclosure or request. 45 C.F.R. 164.502(b)(1). In an interoperable EHR, the adoption of sophisticated features must be taken as a top priority to protect against the disclosure of those portions of the record containing health information that are irrelevant to the disclosure request—that is, if the wide adoption of EHR technology is not to render the "minimum-necessary" standard virtually meaningless.

The Health Information Technology for Economic and Clinical Health Act, H.R. 1, §§ 13101-13424 (HITECH Act), which passed as a component of the economic stimulus legislation, significantly expands security and privacy protections under HIPAA. Prior to HITECH, HIPAA gave individuals the right to request an accounting of disclosures made by health care providers, health plans and other so-called "covered entities" of the requesting individuals' protected health information. HIPAA excluded from the scope of this accounting requirement disclosures made by covered entities to carry out treatment, payment or health care operations. 45 C.F.R. 164.528(a)(i).

The HITECH Act eliminates this exception if the covered entity has made such disclosures through EHR. When it becomes effective on Feb. 17, 2010, HITECH will require an accounting of disclosures to include those made by a covered entity to carry out treatment, payment or health care operations as far back as three years prior to the request. H.R. 1, § 13405(c)(1)(A), (B). The HITECH Act's new accounting duties could add substantially to providers' costs in using EHR technology.

To succeed with the proposed HIT initiatives, legislators, health care industry participants and attorneys should carefully consider the effect and costs of the dueling public policy considerations of health care cost reduction and patient privacy. Perhaps a better solution still is needed if we all are to see realized the goals of a better health care system and reduced costs.

Eric A. Klein is a partner in the Century City/Los Angeles office of Sheppard, Mullin, Richter & Hampton (eklein@sheppardmullin.com). He advises health care companies and private equity funds on acquisitions, technology, financings and regulatory matters. Christine C. Cohn is an associate in that office. She advises physicians and health facilities on regulatory matters, including Medicare reimbursement, fraud and abuse, the Stark law and HIPAA.