THE WALL STREET JOURNAL. ONLINE

Opinion
Industry Rep Calls Patient Privacy 'Overblown' Worry
902 words
30 March 2010
The Wall Street Journal (Online and Print)
WSJO
Letters; A18
English

Thanks to Deborah Peel, M.D., for her March 24 op-ed "Your Medical Records Aren't Secure [http://online.wsj.com/article/SB10001424052748703580904575132111888664060.html]" and for her efforts to protect patient privacy. In 2008, I brought this issue to the floor of the House of Delegates at the AMA, asking that we work to rewrite the Heath Insurance Portability and Accountability Act, a regulation that did not protect patient privacy but only served as a template to deliver the data more consistently to the government. I was voted down. Stunned, I walked back to my seat, only to find any number of reporters as shocked by the lack of support I received as they were to hear this year about the AMA's support of health-care reform.

That was before the stimulus bill and the attempt by the federal government to collect patient data in exchange for money to reimburse physicians for their purchase of an electronic medical records system that will most assuredly not collect clinical data or be a productive tool in the office. To this day, electronic medical records (EMR) continue to sap our energy in time, decrease our productivity and fail to provide any legitimate means of data collection. Not only is patient privacy compromised but the data are administrative data and are not a valid representation of the clinical condition of patients.

This issue remains a conundrum for the profession. Do we say no to the federal government and not engage in taking money for our patients' data? Do we remain our patients' advocate or do we play dead and work for the government? It could be our moral Waterloo if we betray our patients.

Marcy Zwelling-Aamot, M.D.

President

American Academy of Private Physicians

Los Alamitos, Calif.

Dr. Peel states that "The solution is to insist upon technologies that protect a patient's right to consent to share any personal data. A step in this direction is to demand that no federal stimulus dollars be used to develop electronic systems that do not have these technologies."

Her opinion embraces the concept introduced by the Institute for Health Freedom (IHF) in its public comments of March 8 to Health and Human Services Secretary Kathleen Sebelius relating to the Proposed Rule "Medicare and Medicaid Programs: Electronic Health Record Incentive Program." The IHF comments stated that it "strongly recommends that no federal funds be spent on collecting and sharing patients' personal health information electronically without first obtaining patients' consent."

The fact that two leading privacy proponents have now suggested the same measure to ensure patient privacy is an important alert to the federal government and policy makers that such protections should be strongly considered. After all, a patient goes to a doctor to be healed, not revealed.

Robin Kaigh

New York

Dr. Peel does not address all the major security problems. For example, the companies that design electronic medical records assume that the doctors only work within one health-care system. Actually, many doctors work in multiple health-care systems, each of which has its own different brand of electronic medical records. As each brand of EMR demands that the doctors regularly change their passwords, and as each password change occurs on a different random date, most doctors use such trivial passwords that any respectable hacker should be able to access the passwords in less than five minutes. Also, as you wander around any hospital, you are certain to

find a computer terminal that someone has forgotten to log off from, leaving medical information open for all to see.

Stephen Liston, M.D.

St. Paul, Minn.

Dr. Peel seeks to frighten people into believing electronic health records are more vulnerable than paper ones, which is not the case. She fails to acknowledge the important role of the HIPAA in protecting health information, or the extraordinary steps hospitals, health plans and physicians have taken to assure confidentiality. Building upon HIPAA, federal laws adopted this year strongly encourage encryption of data included in electronic health records and have imposed new criminal and civil penalties for violating an individual's privacy.

More importantly, though, if Dr. Peel's prescription for this hyperbolic problem were to be followed, it's actually our health that will be less secure. Burdening patients with the responsibility of deciding what health information should be divulged and what should be shielded from medical professionals brings an infinite array of possible consequences. Would the average patient know what information a surgeon needs in order to perform a complex procedure? It's highly doubtful.

In a broader sense, draconian restrictions on the essential flow of medical information would have society-wide repercussions. It would affect the ability of public health officials to report and track incidences of disease. It would undermine the Food and Drug Administration's capability to monitor the quality and safety of medical products, and product recalls would be hampered.

Perhaps most importantly, medical research into lifesaving cures and treatments would be severely hindered by restricted access to health information. Stymieing the necessary transfer of data contained in one diagnosis, one prescription or one lab test could mean the difference between life and death. That is a very high price to pay in order to address overblown privacy concerns.

Mary R. Grealy

Washington

Ms. Grealy is president of the **Healthcare Leadership Council**, a coalition of chief executives from the health-care industry.

Document WSJO000020100329e63u009ki