Portfolio Media. Inc. | 860 Broadway, 6th Floor | New York, NY 10003 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

EMR Adoption May Be Riskier Than Expected

Law360, New York (February 06, 2013, 1:09 PM ET) -- In 2005, researchers with the RAND Corporation, a nonprofit institution focused on governmental policy and decision making, offered a notably positive assessment of the future impact of health care technology in general, and electronic medical records (EMRs) in particular.

In their 2005 article entitled "Can Electronic Medical Record Systems Transform Health Care?" the RAND analysts found that the adoption of EMRs could create greater efficiencies and improvement in the quality of care, and projected that these efficiencies and improvements were likely to generate more than $81 billion in annual savings to the health care system. Given this optimistic assessment of the impact of EMRs, it was hardly a surprise that in February 2009, the $787 billion financial stimulus package that President Obama signed into law included the "HITECH Act," which offered billions of dollars in government incentives for medical providers who transitioned from paper records to EMRs.

Recently, however, the assessment of EMRs and their utility has begun to grow darker. Just one month ago, a different set of RAND Corporation authors offered an assessment of the impact of EMRs that was strikingly more circumspect and even critical than the one their predecessors had offered approximately seven year before. In their article, this second set of RAND analysts noted that while health information technology such as EMRs still holds the potential for meaningful efficiencies, the results thus far have been a significant disappointment.

According to the RAND authors, EMRs and other forms of "health IT" have not reduced the costs of medical care in the United States, nor have they increased quality of patient care. The reasons for this disappointing trend appear be varied in nature, according to the RAND authors — the culprits may be the lack of interconnectedness and interoperability in EMR systems; the lack of sufficiently widespread adoption of such systems, especially by small hospitals and physician groups; and the prevalence of commercial EMR systems that are not well-designed or usable, and which actually prompt complaints from doctors and nurses that the technology only slows them down. Regardless of the cause, though, the bottom line is clear: At least for the time being, there is reason to question the utility of EMRs and the benefits of the government stimulus program that incentivized their use.

Furthermore, in recent months a still more problematic aspect of EMRs has come to the fore. As events have shown, EMRs not only may lack the utility they originally appeared to promise, but they also appear to provide individuals and entities with a uniquely pervasive and powerful means for committing health care fraud. Indeed, in a development that is both ironic and notable, the most strident expressions of concern regarding the potential abuse of EMRs have come from the very same federal government that vigorously promoted their use just a few years ago.

Three recent events serve to underscore the government's heightened concern regarding the use of EMRs as a vehicle for fraud, and should give pause to medical professionals who adopt and use them. First, in a much publicized letter that was sent on Sept. 24, 2012, to the heads of five associations of hospitals and academic medical centers, Attorney General Eric Holder and Health and Human Services Secretary Kathleen Sebelius noted the potential benefits of EMRs, but then pointed to "troubling indications that some providers are using this technology to game the system, possibly to obtain payments to which they are not entitled."

In referring to "indications" of the abuse of EMRs, the Holder-Sebelius letter appears to have been based at least in part on a front-page article that had appeared two days earlier in the *New York Times*, in which the *Times* notes that EMRs "can automatically generate detailed patient histories, or allow doctors to cut and paste the same examination findings for multiple patients — a practice called cloning — with the click of a button or the swipe of a finger ..."

Similarly, in an investigative report issued on Sept. 15, 2012, the nonprofit Center for Public Integrity reported that medical professionals have increased their billings to the Medicare program by at least $11 billion over the last 10 years, and that the use of more remunerative billing codes "may be accelerating in part because of increased use of electronic health records, which make it easy to create detailed patient files with just a few mouse clicks." Based on these reports, Attorney General Holder and Secretary Sebelius bluntly warned in their letter that "[l]aw enforcement will take appropriate steps to pursue health care providers who misuse electronic health records to bill for services never provided."

Second, as the use of EMRs has grown, so has concern about the ability of hackers and others to infiltrate EMR systems and steal the protected information of individual patients. In October 2011, for example, the Department of Defense announced that an extensive number of backup tapes had been stolen from a contractor for TRICARE, which provides health insurance services to members of the armed services, and that the personal information and medical records of 4.9 million patients treated at military hospitals over the course of 20 years may have compromised as a result.

More recently, Howard University announced in March 2012 that the theft of a contractor's personal laptop compromised the confidential health information of over 34,000 patients, and on April 4, 2012, the Utah Department of Health disclosed a breach of its computer servers that was later determined to have resulted in the apparent theft of the personal information of nearly 800,000 individuals. And, in a twist on the usual scheme involving the theft of EMRs, in August 2012 hackers accessed the medical records of a small medical practice in Illinois, encrypted the records, and demanded a ransom payment in order to unlock the files.

Events like these have increasingly drawn the attention of HHS's Office for Civil Rights, and the scrutiny has focused not just on perpetrators, but on the health care providers who maintain confidential information in EMRs. In fact, in an "Enforcement Highlights" section of the HHS Health Information Privacy website that was last updated on Oct. 31, 2012, HHS notes that one of the most frequently investigated issues regarding medical privacy involves health care providers' "lack of administrative safeguards [for] electronic protected health information."

Third and most recently, the federal government has expressed increasing concern that the medical providers who have shifted to EMRs and are claiming incentive payments under the HITECH Act may themselves be committing fraud. On Nov. 28, 2012, HHS's Office of the Inspector General issued a report in which it noted that while the government expects to pay $6.6 billion in incentive payments to those medical professionals and hospitals that report their "meaningful use" of certified EMR technology, sufficient safeguards are not currently in place to ensure that those medical professionals and hospitals in fact meet the relevant standards. In other words, as HHS-OIG reported, the incentive program for the transition to medical records has been and, absent significant new safeguards, will continue to be vulnerable to making billions of dollars in incentive payments to which providers are not actually entitled.

To be sure, whether EMRs are the new frontier of health care fraud is hardly a foregone conclusion. The response of the American Hospital Association to the Holder-Sebelius letter regarding the "cloning" and upcoding of EMRs vigorously questioned the government's fundamental premise, noting that "more accurate documentation and coding does not necessarily equate with fraud."

The seeming increase of security breaches regarding EMRs has not been correlated to a significant increase in the submission of fraudulent claims, and the potential for health care providers and hospitals to abuse the "meaningful use" requirements and fraudulently obtain incentive payments has thus far been limited to the realm of risk assessments and hypothetical studies. Yet as has always been the case, with technology comes risk. And for the medical providers who adopt EMRs, that risk may include not only a lack of utility or benefit, but also heightened scrutiny, more frequent investigation and even the specter of prosecution by the very government that promoted the switch to EMRs in the first place.

--By Robert M. Radick, Morvillo Abramowitz Grand Iason & Anello PC

Robert Radick is a partner with Morvillo Abramowitz in the firm's New York office.

The opinions expressed are those of the author and do not necessarily reflect the views of the firm, its clients, or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.