

KEYNOTE

What Happened to Do No Harm?

The Bush Administration's ambitious effort to connect millions of electronic health records via a national network poses major risks

BY ROBERT CHARETTE

The Bush administration has embarked on an ambitious national health-care initiative to improve the quality of medical care and stem its rising costs, which just in the last decade have risen to an estimated 15 percent of the gross domestic product (GDP), or about \$1.6 trillion. The centerpiece of this initiative is a national health information network (NHIN) connecting millions of electronic health records (EHRs) for patients. Advocates of EHRs claim that the use of such records could shrink U.S. medical costs by hundreds of billions of dollars annually, reduce the estimated 100,000 lives lost through medical errors and improve the general quality of patient care. Toward that end, President Bush has set up an Office of the National Coordinator for Health Information Technology inside the Department of Health and Human Services.

I find the argument for EHRs very compelling, both from a personal perspective (as a person who has endured surgery several times) as well as a professional one (as a systems engineer who has worked on large-scale software systems in commercial and government sectors). But in this particular case, my risk alarm bells are ringing loudly.

Why? Take, for example, the often intemperate language being used to sell the national health information network. "Paper [medical] records are an utterly irrational national

security risk," and are financially and morally wrong for America, says Newt Gingrich, who has teamed with Senator Hillary Clinton and others to push for EHRs. Other EHR advocates imply that doctors who don't embrace it are harming their patients. I know that to get something moving in politics, over-the-top language is sometimes necessary, but it doesn't help to imply that anyone questioning the value of EHRs is immoral or indifferent to national security or their patients. Further, some government health officials are saying that everyone should "get" with the NHIN program or expect one to be imposed. In my experience, resorting to not-so-veiled threats automatically makes me question the feasibility of the underlying business case.

Advocates of EHRs list a myriad of "challenges" to creating a national health record network— interoperability, privacy, security and making the business case for a decent return on investment to small physician practices that will have to invest in such records to achieve their promise. (For more on this, read ["The Business Case for Paperless Medicine."](#))

Additionally, studies claiming the benefits of a national health information network contain several assumptions. One of the most significant is that networks are composed of EHR systems that are "well-defined and effectively implemented." Yet EHR systems are very complex, human-centered IT systems that must be highly tailored to their operating environment. The HHS department itself has acknowledged that the failure rate for EHR system implementations is 30 percent to 50 percent. Some health-care network providers claim it is as high as 70 percent. So, with thousands of such systems yet to be implemented and interconnected into an interoperable whole, are the benefits being touted realistic?

Questions of Trust

Everyone agrees that any system of networked medical records must be trustworthy. The

medical information in such a system must be complete, free from error and secure, and the confidentiality of the material must be maintained. But how free from error will the conversion of current paper-based medical records to an electronic format be? One study reported a 10.2 percent error rate in transcribing just 2,098 children's vaccine records from paper to electronic records. Other studies indicate that a 2 percent to 5 percent transcription error rate is not unrealistic. Who will be responsible for finding and fixing these types of errors? The doctor? The patient? If someone makes a typo, who would know the difference between Flomax or Volmax?

The need for maintaining privacy is another requirement of the medical network that everyone agrees must be built in from the start. However, even the Department of Defense has a hard time keeping its networks safe from hacking. Even Guidance Software, a leading company that sells forensic software to detect hackers, recently got hacked. Given that 80 percent of U.S. doctors are in practices of eight or fewer physicians, can we expect them to install and keep updated all the security controls required to keep EHRs private?

Psychiatrists especially are alarmed that their patients may not want their records put into EHRs because of the risk of disclosure. Unfortunately, mental illness and even temporary behavioral ailments still carry a societal stigma, and can hinder employment and some types of insurance coverage. If psychiatric patient records are included in EHRs, patients may decide to stop their treatments. Other patients may decide to opt out as well because of the potentially embarrassing information being captured. Are we going to end up with a medical digital divide as a result?

Even assuming a secure network, the availability of EHRs may encourage not-so-subtle

medical redlining by employers and insurance companies. For instance, some insurance companies and employers are promising not to use DNA results in determining eligibility for their health care or benefits plans. The availability of cheap, fast and widespread DNA testing in less than a decade makes such promises suspect. And keep in mind that with access to EHRs and data mining, it is possible to create a genetic profile of a person without ever resorting to DNA.

Who's in Charge?

Another risk that gives me pause is the number of players involved in creating the national EHR network. Not just the 650,000 doctors, 5,800 hospitals, and countless other health-care facilities, but all the players who wish to be involved, from standard bodies to medical associations to EHR suppliers. As of this time, there are 18 bills related to EHRs being contemplated in Congress, each with slightly (or greatly) different consequences for a national system. It has gotten so bad that the HHS has had to politely ask Congress not to be so "helpful."

New organizations are springing up almost weekly, each wanting a say in defining EHR standards. Different groups, from clinical researchers to insurance companies, are lobbying hard for what they believe should be included in EHRs. Requirements creep is bad in any IT project—what is happening here is requirements rush. It is not being overly facetious to suggest that President Bush's 2014 target for EHR adoption may arrive before the first proposed draft of EHR standards is reviewed, let alone agreed upon, if everyone wanting to participate is involved. Are we heading towards a situation where we will end up with everything we asked for but nothing we want?

Similarly, will those who have already invested in EHR systems, such as Kaiser Permanente,

which is investing billions of dollars as we speak, be willing to change to meet a new standard? Especially if the EHR standard requires major revisions of their currently working systems?

Advocates of the national health information network also agree that for it to be effective, there will be a need for massive cultural changes in financial incentives for physicians and in the way they practice medicine. Further, to achieve the postulated cost savings such a network would bring, patients must also assume greater financial responsibility for and decision making concerning their own health care. To expect three simultaneous revolutions in 10 years seems a bit optimistic.

So far, most of the discussion about the cost of the national network—estimated by a 2005 RAND study to be \$156 billion to implement and another \$48 billion a year to operate—has been about what doctors and other health-care providers will need to invest. Very little has been written about the impact on patients, who will ultimately be the ones to foot the bill. Are you willing to pay about \$500 (\$2000 for a family of four) for a network of medical records, along with another \$150 yearly maintenance fee per family member? What about \$750 or \$1000, if the current cost estimates are too low? Will fewer people be able to afford to pay these kinds of premiums for health care? Studies of even small increases in copayments in Medicaid show that they force the poor to go without medical care.

Needed: A Comprehensive Risk Assessment

I have only touched on a very few of the multitude of issues involved in creating an NHIN. What disturbs me most is that I don't see any comprehensive risk management plan for this effort, nor do I see much in the way of a desire to define one. As anyone who has been involved in large-scale endeavors, managing the risks involved from a total enterprise

perspective is absolutely vital to achieving success. If the NHIN is so critical to the nation, if it will radically transform health care in this country, shouldn't there be at least some systemic risk management plan with the risks defined, prioritized and where possible, mitigated?

Since new systems always introduce unexpected problems, such potentially perverse consequences also need to be part of such a plan. Studies have shown that poorly implemented computer physician order-entry systems actually can increase medical errors, for example. What could happen if a large number of poorly implemented EHR systems get interconnected?

Furthermore, paper may kill, but so does not washing your hands. Hospital infections are a large problem because health-care providers routinely fail to wash their hands in between seeing patients. Why isn't there an urgent national effort to address this issue? Instead of waiting for an electronic network to be built, resources need to be directed at mitigating the risks and problems that are unnecessarily costing lives and money today.

I remain unconvinced that the approach currently being taken can develop an effective national health information network, let alone one by 2014. The effort is an unprecedented endeavor, yet the office of the National Coordinator for Health Information Technology is chronically underfunded. Neither the government commitment nor the rhetoric about its importance seem commensurate with the risks or rewards involved.

The creation of this network will, with little doubt, foster a revolution in health care in the United States. But this revolution could be especially messy, given the magnitude of the changes it portends and the new health-care covenant it promises Americans. An enterprise risk management plan would add greatly to the national dialogue and let everyone know what is at stake. By understanding the risks better and then investing the necessary resources for

attacking them aggressively, maybe we can truly gain lasting and fair health-care benefits at an acceptable cost for all Americans.

Robert Charette is the president of Itabhi, a company that specializes in enterprise risk management. He is also the chair of the ISO/IEEE Standard on systems and software engineering risk management. He can be reached via e-mail at charette@itabhi.com. Please send comments to Executive Editor Alison Bass at abass@cio.com.

© 2006 CXO Media Inc.

Dated: April 01, 2006
<http://www.cio.com/archive/040106/keynote.html>