Health Information Technology (HIT): For the Government, or for the Patient?

John V. Mackel, M.D.

Patient-physician interaction is the core element in medical care. All parts of the system should ideally be focused on improving that interaction. Therefore, the principal purpose of the medical record, electronic or otherwise, must be to contribute positively to the interaction.

There is a general principle of computing that states that "computers should only be used where they can be *shown* to improve human performance." The recent medical literature in health information technology (HIT) has not shown this improvement. It has mostly been written by those with a vested interest in its adoption. These include chief information officers and those with an ownership interest in software and hardware companies. The unsurprising result is that HIT is hailed as a miracle drug. If only those pesky physicians would get with the program, all would be wonderful.

The reality of HIT is quite different. The few research papers on the topic show no difference in quality between those practices that use electronic medical records (EMRs) and those with paper records.[1] HIT has also been tried in other countries, the UK in particular, where it has been expensive and disappointing.[2] So, we are left with considerable uncertainty about the utility of the EMR.

This is confirmed by the reluctance of the majority of physicians to adopt it. This reluctance is striking because physicians as a group are generally very ready to adopt new technologies of all kinds. Indeed, some would say we are all too ready! Even when offered "inducements" by the current federal administration (bribes for early adopters and fines for late ones), the majority still do not support the kind of system that our government is attempting to create.[3]

There are major differences between HIT systems. A fundamental difference is between one that is nationally linked, and one that is not. The first is open to access by numerous bureaucracies, governmental and other, and also to unauthorized access or "hacking." The second, unlinked type preserves the privacy of the individual patient record.

Government-Mandated HIT

The linked type has been adopted by our government, with its required characteristics described in the Federal Register (Jan 13, 2010).[3] It is to be forced on all physicians and all patients regardless of their individual wishes. The Administration has also instructed the Federal Trade Commission to hold physicians responsible for any data breaches while those who mandated this system (government) and those who designed and implemented it (HIT industry providers) are held harmless.[4] Such data breaches are virtually guaranteed to occur.

A fundamental problem with a linked system is that no one, including government, can guarantee that it will not be subject to criminal hacking. In fact, given the almost weekly occurrence of hackers accessing various secret and highly protected government and industry databases, it is a foregone conclusion that patient information will be hacked and then misused for a variety of purposes. Wikileaks is a classic example.

The typical medical record contains two types of sensitive information. One comprises financial information such as Social Security numbers, credit card numbers, and banking information useful to identity thieves. The second consists of clinical information that might be useful to employers (chronic back problems) or attorneys (divorces based on STD treatments or paternity issues). The information could be used maliciously to damage a person's reputation ("outing" of gays, identifying patients with STDs, etc.) Or information about children, including names, addresses, and ages, could be the target of predators.

In many cases, sensitive clinical information can be critical in the diagnostic reasoning process. Once patients become convinced that their personal data are no longer private, they may increasingly edit the information they provide to physicians, introducing critical errors into the diagnostic reasoning process.

And this is just the tip of a very large iceberg.

Our government, however, does not seem to attach any importance to this eventuality. Instead it has focused efforts on its ability to access the medical records of all 320 million Americans.

Their linked system allows analysis of these data for Comparative Effectiveness Research (CER). This research method differs from regular medical research in important ways. It adds the factors of cost and appropriateness to regular research.[5] Cost is readily understood. Appropriateness necessarily entails the concept that someone other than patient and physician, such as a government bureaucrat, decides whether a particular plan of management should be approved. These two elements are usually linked.

Appropriate care, however, should be a joint decision of the patient and physician. If the patient is not the final decision-maker, some entity will require the authority to force choices on patients and physicians that they would not otherwise have made. Their decisions could be overridden by bureaucrats prospectively applying, for reasons of cost, a set of rules in a "one-size-fits all" manner. Preauthorizations on a vast scale would be needed. Section 1315 of the Patient Protection and Affordable Care Act (PPACA) gives the HHS secretary the authority to compel physicians to obey or face penalties.[6]

The basic problem with this massive linked data system is that patient privacy has been sacrificed, including both clinically sensitive and financial information, in favor of

budgetary and administrative reasons that focus on rationing. Is there any solution?

Unfortunately, in today's environment where nationwide insurance databases have existed for many years, privacy protection may be available only to self-pay patients. And, with the increasing development of statewide electronic databases, even private information of self-pay patients may be entered into the linked system. Privacy once lost can never be regained.

Patient-Centered HIT

Although it can't stop insurers or medical facilities from entering information into a linked data base, "smart card" technology could enable the clinical benefits of HIT for patients without itself compromising confidentiality.

The fundamental purpose of the medical record is to provide information about past significant events that may influence the diagnosis and/or management of the patient's condition. All physicians know the standard format of presenting complaint, history, family history (genetics), and social history (occupation, personal habits such as smoking, alcohol and drug use, etc.). We physicians mostly need a *summary* of past events, family illnesses, and social history elements, preferably in line-item form.

For example, a typical response to the question "Have you ever had any serious illnesses or hospitalizations" might be: "I had my gall bladder removed in 19xx and a heart attack in 19yy." Patients rarely know, for instance, what type of heart attack they have had. Much more informative for the physician would be the response that "I had an acute full-thickness inferolateral MI with brief ventricular fibrillation," or "I had a gangrenous gall bladder with a small peritoneal biliary leak." We would also like to have a detailed list of allergies, and current medications, again in line-item form.

It is possible to accomplish this readily by using the equivalent of a credit card with an embedded chip. This type of credit card is widely used in Western Europe, and increasingly in the U.S.

Card readers are inexpensive and readily available. They could easily be incorporated into physician offices, hospital wards, and other places of service.

The chip would then have several sections, all in line-item format as follows:

1. Patient identification and financial/insurance information.

2. Past medical history *entered by the responsible health professional at the time.* This would have the brief clinical detail and terminology outlined above, and would include specific drug allergies and side-effects. The attending physician, facility name, and contact information would also be entered.

3. Family history.

4. Social history might be withheld as the most potentially sensitive information, as it can generally be accurately obtained from the patient, if needed, to the extent that he wishes to share it.

5. Specific drug information entered by the pharmacist at point of sale.

Other information occasionally needed would not be on the card. This information is rarely in the patient's possession. It comprises detailed operative reports and discharge summaries, specific test results such as images of ECG tracings, actual X-ray images, etc. These are usually already digitized, on facility computers. A patient-specific access code, such as a fingerprint or individual numeric access code encrypted on the card, could enable access to a facility's information on *that patient only*, providing prompt retrieval of information important to the patient's treating physicians. This of course does not protect the patient's privacy, if the facility has already input information into a linked database to obtain payment. It could, however, overcome the problem, sometimes reported, that the patient's physician is blocked from receiving data accessible to thousands of bureaucrats.

In contrast to the costly, government-certified interoperable EMR systems being urged on physicians by government, the "smart card" approach offers a low-cost, efficient method for accessing the key clinical information, which is controlled by the patient. Some physicians have already implemented such a system in their offices by providing the patient with an encrypted flash drive that the patient keeps and brings to office visits. Flash drives are inexpensive, and physicians might even offer them as a benefit of being a valued patient to the practice.

Conclusions

Insured patients have traded their privacy for third-party payment of medical services provided to them. True patient privacy, if it still exists, does so only for self-pay patients who have treatment encounters only with physicians who do not enter patient information into a linked database system.

The "smart card" approach would offer low-cost access to the benefits of HIT without further compromising the patient's privacy.

The basic choice is between a system that is designed to improve patient care and maintain the privacy of the patient-physician interaction as a primary consideration, and one that is designed for bureaucrats and CER researchers to be used to ration care.

Physicians should choose a system that puts the patient first, rather than bureaucratic budgets or "societal benefits," or the career ladder for CER researchers determining the system design.

John V. Mackel, M.D., attended medical school in the UK system, practiced in Canada and the United States, holds a masters degree in health administration, and teaches health systems and quality in the M.B.A. program at his local university. He also continues to practice primary care. Contact: jmackel@cwcheals.com.

Acknowledgement: Lucas Presson, M.B.A., of Harrison College of Business, Southeastern Missouri State University, provided valuable help with research, as part of his duties as my research assistant.

REFERENCES

1. Karsh B-T, Weinger MB, Abbott PA, Wears RI. Health information technologies: fallacies and sober realities. *J Am Med Inform Assoc* 2010;17:617e623. doi:10.1136/jamia.2010.005637.
2. Wilkinson E. Is the UK health service IT project just too ambitious? *Lancet* 2006;368:1317-1318.
3. Federal Register 2010;75(8):2014 et seq.
4. Koppel R, Kreda D. Health care information technology vendors' "hold harmless" clause: implications for patients and clinicians. *JAMA* 2009;301:1276-1278. doi:10.1001/jama.2009.398.
5. Federal Coordinating Council for CER. Report to the President and Congress; 2009:18.
6. Orient JM. ObamaCare: What is in it. *J Am Phys Surg*. 2010:15: 87-93.