Protecting Patient Privacy in the Information Age

David B. Kendall[*]

The loss of privacy seems to be a foregone conclusion in the information age. Polls show that most Americans believe they have lost all control over the use of personal information by companies.[1] Americans are also concerned about the threats posed by identity theft and fraudulent internet deceptions like phishing.[2] People are learning the hard way to withhold information unless it is absolutely necessary to disclose it. Being discreet has become a survival tool for the information age.

Privacy is a key ingredient of health care, which has yet to see widespread use of information technology. Withholding information from health care providers to protect one's privacy is not good for one's health. For example, a patient who goes to the emergency room with heart trouble may be embarrassed to disclose Viagra use but sharing that information is critical because Viagra is risky for patients when combined with certain heart medications. Patients need to feel safe when sharing personal information; they need to know it will be kept private.

Information technology threatens privacy even as it makes our lives more convenient and our economy more productive. Digitized patient records can be copied and transmitted repeatedly at virtually no cost unlike paper-based records. That is both a problem and an opportunity. It means doctors, health care professionals, and patients themselves can have ready access to complete health care records. At the same time, it means that the number of people who might have access to the most private details of one's life rises exponentially.

A key part of the resolution of this dilemma is to give patients control over who has access to their health care information. This goal could be achieved through an electronic health record (EHR) account. The account would contain all of a patient's clinical information and medical history as well as personal information that patients enter themselves. Patients would establish these accounts through trusted third party organizations called independent health record trusts (IHRTs). IHRTs would release information from a patient's EHR account only with a patient's permission. The transaction could be as simple as a patient giving the doctor's office a magnetic swipe card. Representatives Dennis Moore (D-Kan.) and Paul Ryan (R-Wis.) and Senator Sam Brownback (R-Kan.) have proposed legislation to create IHRTs.[3]

Many advocates for health information technology do not see privacy protection as a necessary precondition for its widespread use. Instead, they see it as secondary issue or as a something that must be balanced with other competing needs. For example, when deciding to let health care providers disclose patient information without patient consent in 2002, the U.S. Department of Health and Human Services "balanced the privacy implications of uses and disclosures for treatment, payment, and health care operations, and the need for these core activities to continue." More recently, a workgroup organized by HHS is trying to "balance the needs between appropriate information protection and access to support" for patients.[4] Although this point of view may sound reasonable, in fact, it poses a false choice between privacy and health care.

To be sure, there are some direct conflicts between privacy and the provision of health care. Federal and state governments require providers to report on a patient's health without asking

[*] David B. Kendall is Progressive Policy Institute's Senior Fellow for Health Policy.

for a patient's permission when it is necessary for purposes such as infectious disease control, law enforcement, or public health monitoring. But requiring patient permission for releasing personal information has been the medical ethic going back to the Hippocratic Oath. Information technology can and should be a tool for protecting patient privacy as well as making health care safer, cheaper, and more convenient.

The Promise of Health Information Technology

The potential benefits from using electronic health records in the health care sector are well established. EHRs can make health care safer, less costly, and more convenient. In 2001, the National Academy of Science's Institute of Medicine stated that the most promising IT systems for managing clinical decisions and operations require an automated system of EHRs containing key patient data.[5] Researchers at RAND have estimated that full adoption of EHR systems would save $81 billion annually.[6] In terms of convenience, EHRs would enable providers and insurers to offer new tools to patients, such as refilling prescriptions and viewing lab results online. Just as the internet has spawned a vast supply of creative ideas and innovative products, so too would an information network for EHRs engender a new generation of computer applications for patients and health professionals.

Much of the key patient information for electronic records has already been digitized. Pharmacies, health plans, and lab companies have already digitized information about prescription drugs, diagnoses, and lab results for their own internal purposes. For example, when pharmacists receive a hand-written or faxed prescription from doctors, they will typically enter the prescription information into a computer system in order to process an insurance claim electronically.

Existing digitized information can be extremely valuable when put to use in the delivery of health care. For example, computers can check automatically for prescribing errors using digitized prescription information. Emergency room physicians can avoid duplicating diagnostic tests when they can see instantly from digital records that a patient's regular doctor has already ordered the necessary tests. This one efficiency measure alone could save upwards of $60 billion each year.[7]

The problem is that existing digitized patient information is not widely available electronically for either patients or doctors to use. It is stranded in isolated computer systems of health insurance plans and other groups. Unless patients have a quick and easy way to give their consent for its use and transfer it electronically, this information will continue to go unused by doctors and their patients.

Existing digitized patient information is already finding a second life as a source for marketing information. For example, a federal law known as HIPAA (Health Insurance Portability and Accountability Act) permits paid advertising directly to consumers based on their prescription histories if a pharmacy, not the pharmaceutical company, carries the message to the patient. On the one hand, a reminder to refill a prescription for a chronic condition is a good health care practice that is no different than reminders from dentists to come in for a regular check-up. On the other hand, when the reminders suggest trying a new drug, patients rightly begin to wonder whether the pharmacist really has the patient's best interest in mind. If patients could choose whether they wished to receive reminders or marketing messages, then they would not feel as if their trust had been violated.

Patient-Controlled Electronic Health Records

With a patient controlled EHR, patients could exercise the right to release the health care information of their choosing. They would have an audit trail of everyone who has seen their EHR account, and they could choose whether or not to open an EHR account in the first place.

To create an appropriate regulatory environment for EHR accounts, the U.S. Department of Health and Human Services would certify independent health record trusts (IHRTs).[8] IHRTs would have fiduciary responsibilities to their account holders for the integrity, security, and the authorized receipt and release of patient data. By law, every health care professional or organization should be required to provide a patient's EHR account with electronic access to any digitized information about a patient. Thus, patients would have a complete version of their medical records when they see multiple doctors, receive tests results from various diagnostic and radiological services, or undergo procedures at hospitals.

IHRTs would function similarly to credit card companies. Credit cards allow consumers to authorize payments on their behalf. The VISA credit card network, for example, enables individual banks and other organizations to issue credit cards while maintaining a broad network that any merchant or any consumer can use. Organizations ranging from WebMD, the online health care service, to the American Association of Retired Persons could become IHRTs. All IHRT accounts would have to be accessible to all doctors and all patients in order to ensure the creation of a broadly used network.

Health plans and employers have already begun to issue personal health records, which are similar to the EHR accounts envisioned in this proposal. According to health insurance industry leaders, by next year, over seventy million Americans will have access to a personal health record that contains records gleaned from medical claims data.[9] Dossia, a collaboration of several large employers including Intel and Wal-Mart, will begin offering employees a personal health record that includes records for medical testing labs and all other sources in addition to records from medical claims.

One potential obstacle for the personal health records offered by health plans and employers is whether patients and their doctors will trust IHRTs to oversee their medical records. Trust is key because no one will participate in a network if they believe it will work against their interests. Physicians and employees are not likely to want to share sensitive information with health insurance plans and employers. Even if health plans and employers create firewalls between themselves and patients' records, they would still be less responsive to the needs of patients than an independent organization that is unencumbered by such restrictions and is beholden directly to patients. Nonetheless, the role of health plans and employers as proponents of change is important because they will be the first to benefit from the elimination of duplicative testing and other savings from electronic health records and are thus a source of financing for IHRT operations.

Under the legislative proposal for IHRTs, an employer-based group like Dossia or a health insurance-based personal health records initiative could apply to be certified as IHRTs. In addition to having fiduciary responsibilities to their account holders, they would have to maintain lifetime access to patient records and ensure portability of EHR accounts for patients who wished to switch to a different IHRT. Different IHRTs could compete for patients based on health care services related to a patient's records. For example, a trust could alert patients with untreatable conditions to clinical trials for experimental therapies or could provide patients with the latest research about their health care problems.

With large databases of medical records comes great potential for research and other uses in both the public and private sectors.[10] People should be able to lend their EHRs anonymously to researchers who will be able to examine their health care experiences and those contained in millions of other digital shadows to figure out new ways to improve health care and lower costs while preserving patient anonymity. Of course, like any other research initiative, IHRTs should be required to disclose their sources of revenue and seek patient's permission over participation in any data-sharing program. This aggregated information will have substantial economic value for both public and private purposes.

Complete Privacy Protection

The success of EHR accounts and IHRT depends on widespread patient approval. If successful, it will provide health IT a solid foundation of support from patients. However, just as patients feel vulnerable when they are exposed in an examination room, patients do not want their confidential health information exposed to prying eyes without their consent. If patients feel they do not have control over who can see their personal health records, patients will try to withdraw from the system. The resulting political backlash from such an incident would hinder the success of any such future initiatives. No system will be foolproof, but patients can balance the risks of losing privacy with the benefits of participating in IT-driven health care, which will only increase over time as medical science advances its understanding of disease, particularly genetic diseases that will require an individual's genetic profile to be included as part of their EHR.

Patient-controlled EHR accounts will give patients the following privacy protections:

1) Voluntary participation.
2) Patient control over access to electronic records.
3) Patient control over segments of particularly sensitive records so that they are not shared in the same manner as the rest of the health record.
4) A list of who has had access to the patient's records.
5) Forbidding employer access to patient records.
6) Disclosure of security breaches to patients.[11]

These protections would be much tighter than the current federal privacy law. HIPAA has many gaps in privacy protection that will expand even further as health information technology becomes more prevalent in the healthcare system. The most significant gap is the absence of a general requirement for health care providers and organizations to seek patients' permission for releasing information, a standard provision of medical ethics for centuries. Instead, HIPAA only requires that providers give patients a disclosure statement about privacy rights, which patients sign only to acknowledge receipt of the disclosure, not to give permission to share their data. Under HIPAA, doctors, hospitals, health insurance plans, and companies that work with providers and plans can see personal medical information without the patient's permission. Although the number of people with access to personal medical information is seemingly self-limiting with paper records, whereas access is virtually potentially limitless with electronic records, the remaining privacy gap under HIPAA could be largely filled by a requirement that any information that an IHRT releases from a patient's EHR account could not be re-released without further patient permission. In other words, the new privacy rules would track the patient's data. As patients' data spread, the new privacy rules would replace the old, less stringent rules by default. An EHR account would enable health care providers and organizations to comply with patient's privacy choices quickly and easily. Nonetheless, a final requirement that all providers and organizations comply with patients' privacy preferences, regardless of whether they actually open an EHR account, likely will be necessary.

Conclusion

Health information technology has clear benefits for patients but the risks for patients of losing their privacy should be minimal. Policymakers can put health information technology to work doing double duty in protecting patients' privacy and making health care safer, cheaper, and more convenient.

[1] Humphrey Taylor, *Most People Are 'Privacy Pragmatists' Who, While Concerned about Privacy, Will Sometimes Trade It Off for Other Benefits*, Harris Interactive, Mar. 19, 2003, http://www.harrisinteractive.com/harris_poll/index.asp?PID=365.

[2] Consumer Reports Webwatch, Leap of Faith: Using the Internet Despite the Dangers 2 (2005), http://www.consumerwebwatch.org/dynamic/web-credibility-reports-princeton.cfm.

[3] *See* Independent Health Record Bank Act of 2006, H.R. 5559, S. 3454, 109th Cong. (2006).

[4] Health Information Technology: Confidentiality, Privacy & Security Workgroup, http://www.hhs.gov/healthit/ahic/confidentiality/ (last visited Mar. 25, 2007).

[5] Comm. on Quality of Health Care in Am. & Inst. of Med., Crossing the Quality Chasm 170 (2001), *available at* http://www.nap.edu/books/0309072808/html/.

[6] Richard Hillestad et al.*, Can Electronic Medical Record Systems Transform Health Care? Potential Health Benefits, Savings, and Costs*, 24 Health Aff. 1103 (2005).

[7] Vincent J. Willey & Gregory W. Daniel, Healthcore, An Economic Evaluation of Use of a Payer-Based Electronic Health Record within an Emergency Department (2006), http://event.on24.com/event/35/62/1/rt/1/images/player_docanchr_5/study.pdf.

[8] Edmund F. Haislmaier, Heritage Found., Health Care Information Technology: Getting the Policy Right (2006), http://www.heritage.org/Research/HealthCare/wm1131.cfm.

[9] Press Release, Blue Cross Blue Shield Association, Industry Leaders Announce Personal Health Record Model; Collaborate with Consumers to Speed Adoption (Dec. 13, 2006), *available at* http://www.bcbs.com/news/bcbsa/industry-leaders-announce-phr-model.html.

[10] Lynn M. Etheredge, *A Rapid-Learning Health System*, 26 Health Aff. 2, (2007), http://content.healthaffairs.org/cgi/content/abstract/26/2/w107.

[11] Privacy Rights Foundation, Patient Privacy Principles, http://www.patientprivacyrights.org/site/PageServer?pagename=PrivacyPrinciples (last visited Mar. 14, 2007).