

Giving Patients Control of Their EHR Data

David Blumenthal, MD, MPP and David Squires, MA

The Commonwealth Fund, New York, NY, 10021 USA.

J Gen Intern Med 30(Suppl 1):S42–3
DOI: 10.1007/s11606-014-3071-y
© Society of General Internal Medicine 2014

The question of whether patients should be able to control the information in their electronic health records (EHR) provokes strong opinions. Some argue that the information rightfully belongs to patients, and they should be able to decide what is recorded and who can access it. Some clinicians, however, argue that because they have a duty to provide their patients with the best possible care, doctors should have unfettered or nearly unfettered access to any information needed to meet that obligation.

In our view, the patient's right to control their own health information dominates. As Dr. Donald Berwick has eloquently professed, clinicians are guests in their patients' lives.¹ And as guests, they must respect the rules and wishes of their hosts, even when those preferences strike caretakers as misguided and even when they may compromise the patient's well-being.

Every day, patients choose (openly or covertly) not to follow clinicians' recommendations—indeed, not to seek care at all. Caretakers have no right to overrule those wishes, even when they profoundly disagree. The idea of force-feeding patients medications or dragging them in handcuffs into the operating room would never occur to us. Assuming patients are mentally competent, we respect their right to control their bodies and their health care fates.

So it should be with their health data. It is perfectly reasonable for patients to be concerned about the deeply personal information contained in their records. Who has access to that information may have ramifications in the patient's life, both inside and outside the health system, that clinicians cannot fathom. The person best positioned to make judgments about the use of their data—and the only person with the right to make that judgment—is the patient.

This view is reflected in the Fair Information Practice Principles adopted in 2008 by the Office of the National Coordinator for Health Information Technology, which underlie the federal government's efforts to encourage privacy, transparency, and accountability for electronic health information. Among these is the principle of *individual choice*—that “individuals should be provided a reasonable opportunity and capability to make informed decisions about the collection, use, and disclosure of their individually identifiable health information”²

With rights, however, come responsibilities. When patients' decisions affect the well-being of others, then the rules change. An individual who has been exposed to Ebola cannot restrict access to that information. A patient who is actively abusing substances should not be allowed to withhold that information from clinicians who may, as a result, unwittingly perpetuate illegal behavior—and endanger third parties who may be affected by the intoxication of the patient.

Furthermore, in controlling their health information, patients assume responsibility for the consequences of their choices. They cannot hold caretakers legally or professionally liable for negative outcomes that stem from lacking information that is purposefully missing or hidden. Patients must accept the attendant risks associated with their data decisions.

However, patients cannot competently assess those risks unless they are meaningfully informed of the consequences of restricting access to their electronic records. This poses a considerable challenge; most patients (and, indeed, most caretakers) currently have little understanding of how health information is shared and used. Kelly Caine et al., in this issue, describe how initially half of the patients participating in the Eskenazi Health study had little or no idea what was contained in their EHR, and none were fully informed about who had access to it.

Furthermore, knowing what is in one's health record is insufficient to give patients a sense of *why* certain caretakers may need certain information. The ways in which caretakers use information are often non-linear and unpredictable. For example, knowledge of drug side effects and their interactions with other medications changes over time. A patient's decision to withhold data about a sensitive medication—such as a psychotropic or HIV-related drug—may have later consequences that neither patients nor clinicians could have anticipated. Beyond this, when evaluating a patient, experienced clinicians often rely on an array of data, including information not obviously related to the current problem, to raise and evaluate hypotheses about diagnosis and treatment.

Communicating to patients the inherent risks and potential consequences of their decisions is a challenge, but has ample precedent in modern medicine: the informed consent process. Clinicians have not always been expected seek their patients' permission when providing invasive care. Only in 1914 did the courts rule that a surgeon performing an operation without the patient's consent commits an assault.³ The need for informed consent has since become ingrained in the medical

Published online December 6, 2014

profession, and clear—though often imperfect—processes for educating patients about their treatment options have become established in policy and law.

Similar processes should be developed for helping patients make informed decisions about their health information. These practices would likely benefit from incorporating shared decision-making techniques, including the use of decision aids and patient testimonies. Patients should also be offered a meaningful range of options. As in the Eskenazi Health study, patients should be able to restrict information for a sensitive condition or for certain providers. Alternatively, they should be able to hide all of their data, or require that they be notified when a provider wants to access their record. Many—perhaps most—will choose to impose no restrictions at all. Whatever their choice, they should be offered the chance to revisit it periodically, as circumstances, scientific knowledge, their own health, and the available technology change. For patients who are not competent to make these decisions, there are standard approaches for the appointment of guardians or the empowerment of health care proxies.

Technologically, electronic record systems' capacity to offer these choices is clearly in its infancy, and will no doubt greatly improve over time. However, some of the technical challenges that Leventhal et al. describe in this issue may take a while to surmount, and so will place limits on the types of control patients can exercise in the near term. As the authors note, given the extraordinary complexity of natural-language processing, it is currently challenging to redact clinicians' notes to hide some diagnoses or conditions.

Finally, there is the question of whether, or in what circumstances, clinicians should be allowed to override their patients' wishes and access information that has been hidden from them. This capability was included in the Eskenazi Health study through the "Break the Glass" feature. While the rules for breaking the glass should be more stringent than in this study—clinicians could do so at any time, for any reason, without the patient being notified—it seems reasonable that the feature should be available in certain circumstances, such as a medical emergency. Built-in safety checks (e.g., for drug-drug interactions) will also likely be developed.

These arguments notwithstanding, some health professionals will continue to believe that their right to treat the patient in a medically professional manner overrides the patient's right to control their health information. Those caretakers should realize that if patients do not trust the health system to protect them, their relationships with their clinicians will suffer, they will withhold information, and the value of the health information contained in the EHR will be undermined. In the long run, clinicians as well as patients will benefit from a health information system that patients feel they can depend on to protect their privacy.

All of these considerations illustrate the long road ahead for patient-controlled health records—but the innovative project described in these articles is a useful step forward. What's needed next is to develop further the technology and processes for informing patients of their choices, carefully put these into practice, and then study the consequences. Continued research on how to inform patients, support their choices, and understand the consequences for their care is essential. And while caution cannot be thrown to the wind, our prejudice should be to give patients a chance to express their views, and then abide by those as best we can.

Corresponding Author: David Blumenthal, MD, MPP; The Commonwealth Fund, New York, NY 10021, USA
(e-mail: db@cmwf.org).

REFERENCES

1. **Berwick DM.** What 'patient-centered' should mean: confessions of an extremist. *Health Aff (Millwood)*. 2009;28(4):w555-w565.
2. Office of the National Coordinator for Health Information Technology. Nationwide Privacy and Security Framework for Electronic Exchange of Individually Identifiable Health Information, Department of Health and Human Services, December 2008.
3. Court of Appeals of New York, 211 N.Y. 125; 105 N.E. 92. <http://wings.buffalo.edu/faculty/research/bioethics/schloen1.html>