Patient Preferences in Controlling Access to Their Electronic Health Records: a Prospective Cohort Study in Primary Care

Peter H. Schwartz, MD, PhD[1,2], Kelly Caine, PhD[3,4], Sheri A. Alpert, PhD, MPA[1,2,3], Eric M. Meslin, PhD[1,2,3], Aaron E. Carroll, MD, MS[1], and William M. Tierney, MD[1,5]

[1]Indiana University School of Medicine, Indianapolis, IN, USA; [2]Indiana University Center for Bioethics, Indianapolis, IN, USA; [3]Center for Law, Ethics, and Applied Research in Health Information, Bloomington, IN, USA; [4]Clemson University School of Computing, Clemson, SC, USA; [5]Regenstrief Institute, Inc., Indianapolis, IN, USA.

INTRODUCTION: Previous studies have measured individuals' willingness to share personal information stored in electronic health records (EHRs) with health care providers, but none has measured preferences among patients when they are allowed to determine the parameters of provider access.

METHODS: Patients were given the ability to control access by doctors, nurses, and other staff in a primary care clinic to personal information stored in an EHR. Patients could restrict access to all personal data or to specific types of sensitive information, and could restrict access for a specific time period. Patients also completed a survey regarding their understanding of and opinions regarding the process.

RESULTS: Of 139 eligible patients who were approached, 105 (75.5 %) were enrolled, and preferences were collected from all 105 (100 %). Sixty patients (57 %) did not restrict access for any providers. Of the 45 patients (43 %) who chose to limit the access of at least one provider, 36 restricted access only to all personal information in the EHR, while nine restricted access of some providers to a subset of the their personal information. Thirty-four (32.3 %) patients blocked access to all personal information by all doctors, nurses, and/or other staff, 26 (24.8 %) blocked access by all doctors and/or nurses, and five (4.8 %) denied access to all doctors, nurses, and staff.

CONCLUSIONS: A significant minority of patients chose to restrict access by their primary care providers to personal information contained in an EHR, and few chose to restrict access to specific types of information. More research is needed to identify patient goals and understanding of the implications when facing decisions of this sort, and to identify the impact of patient education regarding information contained in EHRs and their use in the clinical care setting.

KEY WORDS: Fair information practices; Electronic health records; Patient preferences.

INTRODUCTION

Some experts have suggested that patients should be allowed to exercise control over access by health care providers and others to specific types of personal health information in an electronic health record (EHR).[1] Fair information practices (FIPs) adopted by the Office of the National Coordinator for Health Information Technology and the U.S. Department of Health and Human Services, for instance, support this type of "granular control" of EHR information. A key justification of granular control is to respect the autonomy and privacy interests of patients who may not wish to share specific types of information with certain providers, especially socially sensitive information that may be embarrassing or stigmatizing, for example, regarding sexuality and reproduction, sexually transmitted diseases, drug or alcohol use, and mental illness. Increasing patient control of the EHR may further the goal of encouraging greater patient trust of[2] and participation in the health care system.[1,3]

Efforts to design and implement a system of granular control, however, raise a number of key medical and ethical questions.

- From a medical and ethical perspective, how can a system that provides granular control educate patients and assist them in making decisions that take into account their interest in privacy and confidentiality, but also potential negative impacts on their care? Looking more broadly, how can a system take into account public health goals and providers' desire and responsibility to deliver informed care? Are there situations (e.g., during life-threatening emergencies) where providers should be allowed to override the patients' data-sharing preferences?[4]
- From a technical perspective, how should EHR designers classify types of information in the EHR? How can programmers deal with information contained in narrative text, such as provider notes?[5]

- From a human factor perspective, how can a system efficiently help patients meet their needs and expectations? At what level of granularity should patients control access to their EHRs—the stored data points, classes of data, clinical conditions, or by date, etc.?[4,6]

To address these questions, designers of EHRs need a better understanding of patients' perspectives regarding control of personal information. Previous research has investigated patient preference with respect to sharing EHR data with both health care providers (e.g., physicians) and non-provider recipients (e.g., family members).[6–8] However, none of these studies has investigated patient choices in a health care setting where these preferences were implemented, thereby affecting the actual sharing of their EHR data. This paper presents findings concerning patients' choices for access to personal health information in an EHR in a clinical setting for the first time.

A recent study conducted by one of the authors (KC) showed that patients have varying degrees of comfort with sharing a range of types of information that might be stored in an EHR.[6] The study found that while patients were generally willing to share personal health information with their clinical care providers, especially their primary care physicians, they were more hesitant to share at least some of their personal health information with providers who were not treating them or with other potential recipients of information such as health researchers or family members. Similarly, a survey of patients in Australia and New Zealand found overwhelming willingness to share information with providers who were treating them, but less willingness for that information to be shared with other potential recipients such as administrative personnel, government officials, and health researchers.[8]

Notably, in each of these earlier studies, participants' preferences for sharing health information did not affect how their health information was actually shared. Therefore, a key question remained unanswered: when preferences regarding sharing actually affect what data is shared with providers, what will patients share and with whom?

We investigated this question as part of a larger demonstration project where patients exerted granular control of information in an EHR.[5,9] In an urban public teaching hospital, we asked patients to record their preferences for sharing or restricting data in their EHR with certain recipients (e.g., doctors, nurses, staff), and then implemented these choices to control health care provider access to information stored in each patient's EHR. Finally, we surveyed patients after their preferences had been made and assessed their understanding of the process and their desire to have their preferences implemented.

METHODS

Setting and Participants

This study was approved by the Indiana University Institutional Review Board and was conducted in a hospital-based primary care adult medicine practice in an urban teaching health system. Patients were eligible if they had had at least two visits to their primary care physician in the prior year. When eligible patients presented for care, a research assistant approached the patient in the waiting room, described the study, and assessed their interest. Interested patients were taken to a private room, where the study was described in detail. Risks of the study were described, including the danger that restricting access to data in the EHR might lead to a situation wherein a health care provider might not see information that could be important to their care. In addition, patients were instructed that providers would have the option of viewing all information in the record, including information patients chose to restrict, if the provider felt that it was important to do so. Patients desiring to participate signed informed consent forms. At the completion of the patient's involvement in the study, each was compensated with a $50 gift card.

The research assistant then read a script that again identified the purpose of the study, provided a general description of the types of information included in the EHR, and explained how to use the computer-based program to select preferences for sharing EHR information.

The patient was first shown a heading that asked, "Whose access would you like to restrict?" This was followed by a list of participating clinic providers by name and category (doctors, nurses, and "other staff," which included physician assistants, nurse practitioners, clinical nurse assistants, and medical assistants). The patient could select individual or multiple persons by category. This was followed by a section with the heading, "What information would you like to restrict?" Responses included no information, all information, and five categories of information deemed sensitive and desirable to be restricted: sexually transmitted infections, HIV or AIDS, sexual health and pregnancy, drug or alcohol use or abuse, and mental health. The final section asked, "For what ages would you like to restrict information?" Patients could provide a range of ages, and the system then calculated the relevant dates by using the patient's birth date (a required registration field). Screenshots of the patient preference platform are provided in Leventhal et al. (this issue).[5]

Patients then filled out a survey that assessed their understanding of the EHR and the personal health information contained therein, as well as the process of stating their preferences and controlling access to that information. The questions were drafted, edited, and discussed among co-investigators, a group that included clinicians (PHS, AEC, WMT) and experts in health information technology (KC, SAA, AEC, WMT), human factors (KC), privacy (KC, SAA), survey methodology (AEC), and bioethics (PHS, SAA, EMM). Questions were selected for face validity and were not pilot-tested. There were 10 Likert-style questions, each with the possible answers of "strongly agree," "somewhat agree," "neutral," "somewhat disagree," and "strongly disagree".

Patients' preferences for sharing or restricting access to their EHR data were implemented for a five-month

observation periodin a data-viewing program called CareWeb®, which providers have been using at this hospital since 1977 to access all diagnoses, test results, medications dispensed, vital signs, and other data. Providers were not notified of any information that was redacted unless they clicked on a button on the Careweb screen labeled "Break Glass (Pt Preferences)," at which time any redacted information was displayed.

RESULTS

Demographics

This study was conducted from August through December of 2013. During the study period, 139 eligible patients were approached, and 105 (75.5 %) patients were enrolled and preferences were collected from all105 (100 %). The demographics of enrolled patients are displayed in Table 1. Of the 105 patients, 104 (99 %) had sensitive information in their EHRs, meaning that it was judged to fall within at least one of the five categories identified in advance. Fifty-two (49.5 %) patients had data related to HIV or an HIV test.

Patient Preferences for Sharing EHR Data with Doctors, Nurses, and Other Clinical Staff

Sixty patients (57 %) chose to provide all listed providers with access to all personal health information in their EHR. Forty-five patients (43 %) chose to limit the access of at least one provider to EHR data.

Thirty-six patients (34.2 %) restricted the access of at least one provider to ALL personal information in the EHR (i.e., no partial access was granted to any sensitive information within the five categories or information within a specific time period) . In other words, these patients controlled the access to their EHR as a block of data.

Tables 2, 3, and 4 provide information regarding preferences for sharing EHR data by patients who either granted complete access or blocked all access to all of their data as a single block. Thirty-four (32.3 %) participants denied access to all listed individuals of at least one provider/employee type (i.e., doctors, nurses, or other staff), 26 (24.8 %) patients blocked access by all doctors and/or nurses, and five patients (4.8 %) denied access to all doctors, nurses, and other staff to view any of their EHR information.

Nine patients (8.6 %) restricted the access of at least some providers to a subset of the personal information in the EHR (Table 5); that is, these patients took advantage of the opportunity to exercise granular control over personal information in the EHR. Six patients (5.7 %) restricted the access of at least some providers to at least one sensitive type of information, and four patients (3.8 %) restricted access to at least some information based on time period.

All 105 enrolled patients responded to the survey that was administered after their preferences had been accepted, in which they were asked to provide their opinions regarding the preference process and control of access to the EHR. As shown in Table 6, a vast majority of participants agreed or strongly agreed with the statements that they understood the following: "what an electronic health record is" (90.4 %), "what information is in my electronic health record" (96.2 %), and "who can view my electronic health record" (96.2 %). A vast majority also agreed

Table 1. Participant Demographics

	Number of Participants (%)
Gender	
Male	31 (30 %)
Female	74 (70 %)
Age (years)	
18–30	2 (2 %)
31–45	16 (15 %)
46–64	62 (59 %)
≥65	25 (24 %)
Race	
White	46 (44 %)
Black	48 (45 %)
Unknown	11 (10 %)

Table 2. Choices by Patients Either Granting Access or Blocking Access to ALL EHR Information (no partial access granted, i.e., did not exercise "granular control" over particular types or time periods for EHR data) (*n*=96): Number of Patients Granting Access to Specific Numbers of Doctors, Nurses, or Staff

No. of individuals granted access			No. of patients who chose this option
Doctors	Nurses	Staff	
0	0	0	5
0	1	0	1
0	1	1	1
0	2	1	1
0	0	1	4
0	0	4	1
1	0	0	2
1	0	1	1
1	1	1	1
2	0	0	1
0	All	1	1
1	All	0	1
0	All	0	1
0	All	All	1
All	0	0	3
All	2	0	1
All	0	1	2
All	1	All	1
All	0	All	1
All	All	0	6
All	All	All	60

Table 3. Number of Patients Granting Access to All/Some/No Participating Doctors vs. Nurses and Staff

		Access granted to		
		All doctors	Some doctors	No doctors
Access granted to:	All nurses and staff	60	0	1
	Some nurses and staff	11	3	10
	No nurses and staff	3	3	5

or strongly agreed that the process of stating their preferences was easy to do (95.2 %), that undergoing this process made them feel more comfortable with providers viewing the records (97.1 %), that it was acceptable for them to prevent some providers from seeing parts of their EHR (93.3 %), and that it was a good thing for patient to have control over who sees specific electronic health information (94.3 %). Of note, patients were in various levels of agreement with the statement, "Preventing some providers from seeing parts of my electronic health record could affect my relationship with them": 48.6 % agreed or strongly agreed, 14.3 % were neutral, and 34.2 % disagreed or disagreed strongly.

DISCUSSION

When given the opportunity to limit access to some portions of the personal information in their EHRs by at least some health professionals, a significant minority of patients (43 %) chose to do this, and 4.8 % restricted all providers' access to all EHR information. This result is particularly important because it is the first study of granular patient EHR data-sharing preferences in a clinical setting where their choices affected the ability of their primary care providers to access information in the EHR. Since patients received limited education

Table 4. Number of Patients Who Restricted Access of Doctors, Nurses, and/or Staff to ALL Personal EHR Information

	Number (%)
Restricted access by doctors	
Restricted access by ALL doctors	16 (15.2 %)
Allowed access by just one or two doctors	6 (5.7 %)
Restricted access by nurses	
Restricted access by ALL nurses	20 (19.0 %)
Allowed access by just one or two nurses	6 (5.7 %)
Restricted access by staff members	
Restricted access by ALL staff members	21 (20 %)
Allowed access by just one or two staff members	11 (10.5 %)

Table 5. Choices by Patients Who Restricted Access for at Least Some Doctors, Nurses, or Staff to Part of Their Personal Information in the EHR

Restricted access to	Number of patients (%)	Patient ID#s
Time period	4 (3.8 %)	#s 4, 5, 6, 7
Mental health	4 (3.8 %)	#s 1, 2, 3, 7
Drug/alcohol use	3 (2.9 %)	#s 1, 8, 9
Sexually transmitted infection	1 (1.0 %)	#1
Sexual health/pregnancy	1 (1.0 %)	#1
HIV	0 (0 %)	

regarding the content and use of the EHR, their choices can be understood as a "baseline" that may indicate a starting point for educational efforts necessary for future implementations of granular control.

Our finding that a majority of patients (57.1 %) chose not to impose any limitations on access for any listed health care providers is in line with previous findings. Whiddett et al. (2006) found that more than 75 % of patients would be willing to share general nonsensitive personal information in their EHR with a doctor or practice nurse. When it was specified that the information could include potentially sensitive data (e.g., regarding sexually transmitted diseases or mental health), 70 % agreed to allow access to a doctor or practice nurse.[7] In another study, 86 % of HIV patients said that they would be willing to share personal health information through an electronic record with their primary HIV care provider, 78 % agreed to share that information with other clinicians in the same clinic, and 78 % agreed to share the information with other health care providers such as emergency or hospital personnel.[8] In a third study, this time of patients without sensitive information in their EHRs, 100 % said that they would share less sensitive items with their primary care physician, while 78 % would share highly sensitive items. For patients whose EHR contained sensitive information, 95 % would share nonsensitive items and 76 % would share highly sensitive items.[6]

These results, like ours, suggest that many patients believe that their providers have good reason to see such electronically stored health information and can be trusted to use it responsibly, even when it contains potentially sensitive information. Interpretation of our results is limited, since we do not have information about patient understanding or reasons for choices, and thus it may be that allowing providers to view the records could have been a "default" choice that reflected avoidance of making an active choice. In addition, it is important to consider that a majority of our patients may have allowed complete access to all listed providers because the patients may have known the providers for some time (an inclusion criterion was that the patient had made at least two visits to the clinic in the previous year). This personal experience may have increased patients' comfort level with allowing

Table 6. Patient Responses to the Post-Preference Survey

	Strongly agree	Somewhat agree	Neutral	Somewhat disagree	Strongly disagree	Don't know or can't say
I understand what an electronic health record is	72 %	18 %	3 %	4 %	3 %	0 %
I understand what information is in my electronic health record	80 %	16 %	1 %	1 %	2 %	0 %
I understand who can view my electronic health record	88 %	9 %	2 %	0 %	2 %	0 %
Today I underwent a process where I decided who could access my electronic health record	90 %	9 %	0 %	0 %	1 %	0 %
I found the process of making my preferences known easy to do	89 %	7 %	2 %	2 %	0 %	1 %
This process made me feel more comfortable about providers seeing my electronic health records	89 %	9 %	1 %	1 %	1 %	0 %
This process made me feel that only those who should have access to my electronic health record do have access	90 %	6 %	2 %	1 %	2 %	0 %
It is okay for me to prevent some providers from seeing parts of my electronic health record	82 %	11 %	4 %	2 %	1 %	0 %
Preventing some providers from seeing parts of my electronic health record could affect my relationship with them	34 %	14 %	14 %	13 %	21 %	3 %
It is a good thing for patients to have control over who sees specific electronic health information	85 %	10 %	3 %	1 %	2 %	0 %

the employees and providers to view all EHR information. A recent Cochrane Review has shown that such trust has far-reaching effects, since it is associated with increased patient satisfaction, adherence to treatment, and continuity of care.[10]

It is notable that most of the patients in our survey agreed that it was acceptable to prevent some providers from seeing parts of the EHR, that it was a good thing for patients to have control over who sees specific electronic health information, and that the process of making choices regarding access by providers made the patient more comfortable with others viewing the EHR. On the other hand, almost half of the patients also agreed or strongly agreed that preventing a provider from seeing parts of the EHR could affect their relationship with the provider. This may suggest that patients are concerned about the possible impact that restricting access to the EHR could have, and it may have been an additional reason why at least some patients did not impose limits on any providers or employees. Managing and addressing such concerns will be an important goal of any initiative to implement more widespread granular control of EHRs.

Among patients who chose to limit access to their medical records, a large majority (36 of 45, or 80 %) limited access to the entire EHR rather than parts of it. There are many possible reasons for this choice, including the relative ease with which the patient preference program interface allowed patients to limit access to all personal data in the EHR, as they could do so by checking a single box. If a patient was concerned about sharing one particular type of information and was unsure about how to characterize it, they might simply choose to restrict access to all data. Compared to restricting access to just a single type of information such as sexual history, for instance, a global restriction on access to EHR data could carry greater risk of causing significant negative consequences for an individual's health care.[11] These potential dangers of restricting access to providers or employees at the clinic may not have been apparent to patients, given the relatively limited training that they received regarding the information stored in EHRs and its use in clinical care. In addition, our finding that

15.2 % of patients blocked all access to the EHR for all physicians participating in the study is at odds with the finding in a previous study that 100 % of patients, many from the same health system that we studied, would share nonsensitive data with their primary care physician.[6] Future research should investigate the impact of additional education as well as the user interface design on patient choices to restrict access to all or part of their information.

Of the 36 patients who blocked access to the entire EHR to at least some providers, 34 of them (94.4 %) restricted access to *all* members of at least one group of providers/employees (i.e., doctors, nurses, or staff). Five denied access to all listed doctors, nurses, and staff for viewing any of the information in the EHR, while 26 blocked access to all doctors and/or nurses. Such choices raise important questions that should be studied in future research. Did patients who blocked access to all providers/ employees actually intend to do this (e.g., did any who chose to block access believe that they were granting access?)? Do patients who block access to all doctors envision that the provider can provide adequate care without referring to any previous information stored in the EHR? Do patients who block access to all nurses or staff have an adequate understanding of the use of the EHR by these members of the clinic? For instance, are patients aware that nurses access the EHR to issue new prescriptions for medications that the doctor has previously prescribed? It is possible that patients would be willing to accept the risk that they take on by restricting access to some of their information, particularly if that access is restricted for non-clinicians working in a medical practice. Such questions about patient understanding and intent must be addressed in future research.

While it important that patients' privacy needs are respected, there would be significant risk in implementing a system that simply empowers what might be uninformed or unreflective choices regarding the restriction of access to EHR data. Our findings thus re-emphasize the need for any system of granular control to be coupled with an efficient and meaningful system for educating patients on the type of information

included in the EHR, who uses it and why and how, and the potential impacts of restricting access to data.[4]

Like all studies, our work has limitations that warrant consideration. First, we utilized a simple patient interface for stating choices, and there was no educational intervention regarding the content and use of data in the EHR beyond simply listing types of information that it contains. Any wider implementation of a granular control system must involve a more carefully designed interface and educational program, along with the ability for patients to access their own EHR data, in order to help patients make informed decisions that can protect their privacy interests while also ensuring that they receive excellent health care. Second, the study was conducted at a single clinic that serves a population of low socioeconomic status, and thus our results cannot necessarily be generalized to other patient populations. Future work should investigate the opinions and responses of patients in other practices and with different demographic characteristics. Third, this project studied patient preferences only with regard to access of information by providers and employees of a primary care clinic, not in other settings such as hospitals, emergency rooms, insurance companies, or myriad other secondary users of clinical information. Fourth, this study did not assess patient preference regarding granular control of EHR data for research use rather than clinical care.

In summary, this is the first study of choices among patients with regard to restricting access by primary care providers to personal EHR data when those choices affect access in a real-life clinical setting. Many patients chose not to restrict access for any doctors, nurses, or staff, and most of the patients who did restrict access did so by blocking access to all of the personal information in the EHR rather than to just sensitive information or specific date ranges. More research is needed to identify patient goals and understanding in making decisions of this sort, and to explore the impact of various types of patient education regarding the information that is contained in the EHR and how it is used in clinical care and beyond. In addition, further research is needed with respect to the impact of the interface design on patient choices regarding granular access to personal EHR data.

Corresponding Author: *Peter H. Schwartz, MD, PhD; Indiana University School of Medicine, 410 West Tenth Street, Suite HS3100, Indianapolis, IN 46202, USA (e-mail: phschwar@iu.edu).*

REFERENCES

1. President's Council of Advisors on Science and Technology. Report to the President realizing the full potential of health information technology to improve health care for Americans: the path forward. Washington, DC: Executive Office of the President.; 2010.
2. **Pritts J.** The importance and value of protecting the privacy of health information: roles of HIPAA privacy rule and the Common Rule in health research. Inst Med. 2008.
3. **Undem T.** Consumers and health information technology: a national survey. 2010; http://www.chcf.org/~/media/MEDIA%20LIBRARY%20Files/PDF/C/PDF%20ConsumersHealthInfoTechnologyNationalSurvey.pdf. Accessed Sept. 14, 2014.
4. **Meslin EM, Alpert SA, Carroll AE, Odell JD, Tierney WM, Schwartz PH.** Giving patients granular control of personal health information: using an ethics 'points to consider' to inform informatics system designers. Int J Med Inform. 2013;82(12):1136–43.
5. **Leventhal JC, Cummins JA, Schwartz PH, Martin DK, Tierney WM.** Designing a system for patients controlling providers' access to their electronic health records: organizational and technical challenges. JGIM. In press (Supplement).
6. **Caine K, Hanania R.** Patients want granular privacy control over health information in electronic medical records. J Am Med Inform Assoc. 2013;20(1):7–15.
7. **Whiddett R, Hunter I, Engelbrecht J, Handy J.** Patients' attitudes towards sharing their health information. Int J Med Inform. 2006;75(7):530–41.
8. **Teixeira PA, Gordon P, Camhi E, Bakken S.** HIV patients' willingness to share personal health information electronically. Patient Educ Couns. 2011;84(2):e9–12.
9. **Tierney WM, Alpert SA, Byrket A, et al.** Provider responses to patients controlling access to their electronic health records: a prospective cohort study in primary care. JGIM. In press In press (Supplement).
10. **Rolfe A, Cash-Gibson L, Car J, Sheikh A, McKinstry B.** Interventions for improving patients' trust in doctors and groups of doctors. Cochrane Database Syst Rev. 2014;3, CD004134.
11. **Kozubal DE, Samus QM, Bakare AA, Trecker CC, Wong H-W, Guo H, Cheng J, Allen PX, Mayer LS, Jamison KR, Kaplin AI.** Separate may not be equal: a preliminary investigation of clinical correlates of electronic psychiatric record accessibility in academic medical centers.". Int J Med Inform. 2013;82(4):260–7.