Patients want granular privacy control over health information in electronic medical records

Kelly Caine,[1] Rima Hanania[2]

[1]School of Computing, Clemson University, Clemson, South Carolina, USA
[2]Department of Psychological and Brain Sciences, Indiana University, Bloomington, Indiana, USA

Correspondence to
Kelly Caine, 314 McAdams Hall, Clemson, SC 29634, USA; caine@clemson.edu

Received 15 October 2012
Accepted 21 October 2012
Published Online First 26 November 2012

ABSTRACT

Objective To assess patients' desire for granular level privacy control over which personal health information should be shared, with whom, and for what purpose; and whether these preferences vary based on sensitivity of health information.

Materials and methods A card task for matching health information with providers, questionnaire, and interview with 30 patients whose health information is stored in an electronic medical record system. Most patients' records contained sensitive health information.

Results No patients reported that they would prefer to share all information stored in an electronic medical record (EMR) with all potential recipients. Sharing preferences varied by type of information (EMR data element) and recipient (eg, primary care provider), and overall sharing preferences varied by participant. Patients with and without sensitive records preferred less sharing of sensitive versus less-sensitive information.

Discussion Patients expressed sharing preferences consistent with a desire for granular privacy control over which health information should be shared with whom and expressed differences in sharing preferences for sensitive versus less-sensitive EMR data. The pattern of results may be used by designers to generate privacy-preserving EMR systems including interfaces for patients to express privacy and sharing preferences.

Conclusions To maintain the level of privacy afforded by medical records and to achieve alignment with patients' preferences, patients should have granular privacy control over information contained in their EMR.

INTRODUCTION

Recent advances in technology have the potential to transform healthcare in the USA and around the world. The widespread adoption of health technologies such as electronic medical records (EMRs) has the potential to improve coordination of care, healthcare quality, patient engagement, and many other areas of healthcare. This vision, as described in a recent report by the President's Council of Advisors on Science and Technology is for 'a national health IT ecosystem in which every consumer, doctor, researcher, and institution has appropriate access to the information they need'.[1] The vision is based on the assumption that the collection, aggregation, analysis, and dissemination of health information, specifically health information that is stored electronically, may be used to make healthcare more integrated and well-coordinated, which can in turn result in better patient outcomes and lower healthcare cost. There is little disagreement that this is a laudable and eventually realistic goal. There is also little disagreement that there are many barriers which must be overcome before this goal is realized.[2]

One barrier that has been identified in the acceptance of health technologies such as EMRs is concern about privacy and security.[2 3] The introduction of information technology into a system is widely understood to fundamentally change the nature of individual privacy because it enables collection and storage of data on a scale not possible using non-electronic methods.[4] Personal information captured in information systems, as opposed to systems existing before the widespread implementation of information technology (eg, paper-based filing systems), may be reproduced infinitely, transmitted instantaneously, used in ways formerly unimaginable (eg, data mining), introducing new problems of privacy and security. Thus, unless health information systems are carefully designed to preserve and protect patient privacy to at least the same level of non-information-technology-enabled systems (eg, paper-based system), their introduction may vastly decrease the level of individual privacy afforded during and beyond a healthcare encounter. Furthermore, and of specific interest in this research, the growth of health information exchange means that increasingly patient records will be made available across a much wider range of healthcare settings, thus increasing the number of potential recipients (eg, healthcare providers at a hospital that the patient has never visited) of electronically stored individual health information.[5] Together, these two issues necessitate close consideration of potential privacy issues. Indeed, controlling and sharing access to information in a personal health record (PHR), a technology that is similar to an EMR, has been noted as an area in great need of additional systematic investigation.[6]

BACKGROUND AND SIGNIFICANCE

One framework for the maintenance of individual privacy is the fair information practices (FIPs) or FIP principles. The term FIP is used to describe a series of documents on practices/principles designed to ensure that 'the use of technologies sustains and does not erode, privacy protections relating to the use, collection, and disclosure of personal information'. These principles or practices recognize that the use of information technology fundamentally changes the nature and scale of privacy consequences. FIPs are meant to maintain the level of individual privacy afforded by existing non-information-technology-enabled systems (ie, an IT system should provide an equivalent level of individual privacy as a paper-based system).

The FIP principles, described by the Office of the National Coordinator for Health Information

Technology and the US Department of Health and Human Services, are as follows: individual access, correction, openness and transparency, individual choice, collection, use and disclosure limitation, data quality and integrity, safeguards, and accountability.[7] Based on FIPs, individuals should have access to their health information, knowledge of what is in their record, the ability to correct errors, control over whether information is collected and, if collected, for how long the information is stored, and know with whom the information is shared. The embodiment of these requirements within an EMR system is one of the goals of this research.

An objective of many in the health information technology community, notably the Office of the National Coordinator for Health Information Technology and the US Department of Health and Human Services, is to spur the design and implementation of a privacy-enhanced EMR based on FIPs. A key human factors question that emerges from the integration of privacy-preserving FIPs with EMRs is, at what level of granularity do patients want to make 'individual choices' about the collection, use, and disclosure of their health information? Does 'individual choice' mean that patients wish to exert control over the individual recipients and elements of an EMR? What constitutes a recipient?—A hospital system? An individual healthcare provider? To a patient, does individual choice mean sharing an entire EMR record? A portion of the record? Data about a specific condition? Results from an individual test? To answer the question of whether patients want to share their whole electronic health record or portions of their record, and to determine the patterns of sharing preferences across recipients and record types, we designed a study to elicit patients' future sharing and privacy goals and aimed to understand their aspirations for data-sharing capabilities and specific privacy concerns related to the sharing of health information.

This work aimed at examining the human factors of privacy as they relate to patients' preferences for sharing EMR data with a variety of potential recipients. We used a sharing-preferences card-sort task (described in detail in the 'Methods' section) to determine patients' preferences for sharing EMR information across recipients and across information types. In the following section we describe the materials and methods we used to meet this objective.

MATERIALS AND METHODS

This study is part of a larger project investigating patient sharing and access preferences to EMR with the aim of designing a user interface with which patients can access their own EMR and manage the way in which data in their EMR is shared with others. The focus of this portion of the project is to understand patients' desires for sharing health information. Participants in this study completed a questionnaire, three card-sorting exercises and a semistructured interview. We report here data from the questionnaire, card-sort task and portions of the interview that are specific to the question of what information participants wanted to share with each of several potential recipients. The entire study was approved by the Indiana University institutional review board.

Participants

Thirty adults receiving healthcare in central Indiana were recruited for the study. Patients fulfilled the following criteria: they were current or recent patients with health records in the Indiana Health Information Exchange, particularly those with highly-sensitive health information (as discussed below), with as wide a range of demographics (age, race, and socioeconomic status) as possible.

Participants were recruited through one of three methods. Thirteen participants were recruited from the Indiana Network for Patient Care (INPC), the country's largest health information exchange of data from hospitals, physicians' offices, pharmacies, and laboratories. Patients in the INPC who were eligible for this study were identified and recruited by the research recruitment office of the Indiana Clinical and Translational Sciences Institute (CTSI) through a network of trained recruitment personnel called ResNet. Once identified, patients were approached by ResNet personnel at their clinic appointments, and were told about the study, and invited to participate. In addition to the INPC patients, 13 participants were recruited by the CTSI recruitment office from a volunteer recruitment registry for residents in Central Indiana called INResearch. This registry links volunteers with various health conditions to investigators needing participants. The CTSI recruitment team identified a list of potentially eligible individuals from INResearch, and emailed notification to the list of individuals, indicating that they might be contacted for a research study. Those people who expressed interest were then contacted for scheduling. Four additional participants were recruited through flyers posted on the Indiana University Indianapolis campus.

Defining highly-sensitive medical records

Central to the question of privacy within a medical record is whether some health information might be considered 'more private' and thus less likely to be shared. Specifically, we were interested in understanding whether patients consider some information sensitive and therefore may not want to share it in the same way as they would 'less-sensitive' information. In this study, we used the definition of sensitive information listed in the National Committee on Vital and Health Statistics' (NCVHS) recommendations about individual control of sensitive health information accessible via the Nationwide Health Information Network.[8] This letter listed five categories of health information that are considered by NCVHS to contain sensitive information: domestic violence, genetic information, mental health information, reproductive/sexual health (including sexual activity, sexual orientation, sexually transmitted disease, adoptions, abortions, and infertility), and substance abuse. Participants who had items in their own medical history that fell under one of the sensitive information categories were purposefully oversampled to ensure we obtained a sample where all sensitive categories were represented. Information about sensitive health categories in medical records was accessed by CTSI staff only, and just for recruitment purposes. We considered health record sensitivity a grouping variable for the purposes of analysis.

Materials

Questionnaires

Participants completed a demographics questionnaire and a technology experience questionnaire. These included questions about age, race, educational background, and household income, as well as questions assessing health status and computer experience. The questionnaires were administered in paper and pencil form.

Sharing-preferences cards

A card-sort task was used to assess patients' preferences for sharing EMR data with a variety of potential recipients. Participants chose which EMR items (on cards) they would share with which recipients (also on cards). The *recipient* card set contained 14 possible

recipients of EMR data, including various types of healthcare providers and non-healthcare-related individuals. The *item* card set contained 11 types of health information items that could exist in an EMR, including all the sensitive information items.[8] Sexual history was listed separately from reproductive health to distinguish the two types of information. The complete list of *recipients* and *items* from the two card sets is listed in table 1 in the order in which they were presented to participants in the card-sort exercise. The cards were printed on colored card-stock paper and cut to 2.5×6.6 square inches. One set was on yellow paper, the other on green to allow easy distinction of recipients and items.

Procedure

The procedure was the same for all participants. Participants gave their informed consent before beginning the session. Each session was conducted with a single participant and took 3 h, during which the participant completed the following tasks in fixed order: paper-and-pencil questionnaires, two *information architecture* card-sorting tasks which relate to the user-interface design portion of the larger study, a semistructured interview to understand patient attitudes toward EMRs, and a *sharing-preferences* card task. Only two questionnaires and the *sharing-preferences* card task are relevant to the questions examined in this paper and will be discussed here.

The *sharing-preferences* card task was conducted to identify which types of health information participants wanted to share with which potential recipients. Participants sat at a table, and the researcher introduced the task by saying: 'In this card exercise, I will ask you what type of information in a medical record you would want to share with different potential recipients. Here are types of items that might appear in a medical record'. The *item* cards (listed in table 1) were placed on the table in front of the participant one by one, in two columns, with the less-sensitive items (first five in table 1) placed in the left-hand column, and sensitive-health-information *items* (the last six items in table 1) placed in the right-hand column. As each card was placed on the table, the researcher described the item on the card. For example, the researcher placed the contact information card and said 'There might be demographic information and contact information, such as address or telephone number, in a medical record'; and so on. The sensitive-health-information items were introduced in the same way with a comment by the researcher that these were specific examples of what some people would consider more sensitive information. This was done to ensure that all participants thought seriously about the types of information they might have in a record and the relative sensitivity of some information. After all the item cards were on the table, the interviewer presented a *recipient* card and asked the participant to point to the *items* that the participant would want to share with that recipient. For example, the primary physician card was placed next to the *item* cards and the participant was asked, 'Which of these health information items would you want your primary physician to have access to?' Participants were encouraged to think aloud as they performed this task. This process was repeated for all recipient cards in the order seen in table 1. Responses were recorded on paper and on an audio recorder.

RESULTS

Demographics

Participants' demographic characteristics are displayed in table 2. Mean age of the participants was 45.93 (SD=11.95), with the majority of participants (70%) aged >45 years. This might be a reflection of the fact that we targeted a population

Table 1 Card-sort items and description (as provided to participant)

Card items	Description
Recipient	
Primary physicians (current)	Generalists
Mental health providers	Psychiatrists or counselors
Pharmacists	(Intentionally blank)
Government agencies	State health department, court system
Health insurance companies	(Intentionally blank)
Specialized physicians involved in care	Cardiologist, endocrinologist, allergist
Nurses and assistant medical staff	(Intentionally blank)
Alternative-medicine therapists	Acupuncture, massage, herbal therapy
Administrative personnel	Front desk, scheduling, billing
Researchers	Education, medical or pharmaceutical
Home-care and rehabilitation providers	Nursing care, physical/occupational therapists
Physician (not treating you)	(Intentionally blank)
Family and close social network	Spouse, close family members or friends
Emergency medicine providers	Emergency care physicians, paramedics
Item	
Contact information and demographics	Address, telephone number, race
Information relevant to current condition	Illness, symptoms, hospitalization
Medications	Prescribed and over-the-counter medicines
Recent test results	Pulse, blood pressure, weight, height
Past medical history (unrelated)	Previous injuries or illnesses
History of substance abuse*	Records of drug or alcohol abuse, treatment
Mental health information*	Psychiatric diagnosis, suicide attempts
Sexual health information*	STDs including HIV, sexual orientation
Records relating to domestic violence*	Fear of partner, suspicious physical injury
Reproductive health records*	Infertility, abortions or miscarriages, adoption
Genetic information*	Paternity testing, genetic tests

*Indicates 'sensitive' health information as defined by the National Committee on Vital and Health Statistics.
STD, sexually transmitted disease.

Table 2 Participant demographics, health status and technology experience

	Overall (N=30) (%)
Medical record	
Highly-sensitive	70
Less-sensitive	30
Gender	
Male	27
Female	73
Age	
18–30	17
31–45	13
46–64	63
≥65	7
Education	
High school or less	37
Beyond high school, <4 years college	33
Four-year college graduate or more	30
Race	
White, non-Hispanic	70
African-American	23
Multiracial	7
Household income	
<$5000	20
$5000–$14999	13
$15000–$19999	17
$20000–$49999	20
$50000–$59999	10
$60000–$99999	3
≥$100000	17
Health status	
Poor	17
Fair	20
Good	33
Very good	20
Excellent	10
Computer experience	
Yes	87
No	13
Internet use	
Never	21
1–10 h/week	27
11–15 h/week	14
>15 h/week	38

of participants with sensitive health information. Indeed, 70% of our participants (21/30) fell into that sensitive health information category, and 37% of the participants reported *poor* to *fair* health status. Most participants with highly-sensitive health records fell into multiple sensitive health categories, with the full range of sensitive-health information well represented. By chance, most participants (73%) were female. Around two-thirds of the participants were non-Hispanic whites; the rest were African-American or multiracial. They covered a range of socioeconomic backgrounds, with half of the participants having a household income <$20 000, and 17% over $100 000. The participants were well distributed according to educational background, ranging from around one-third with a high-school education or less, to around one-third with at least a 4-year college degree.

A vast majority of the participants (87%) had computer experience, with many hours of internet use. Over half (52%) used the internet for more than 11 h a week. However, there was a range of computer experience; 13% reported not having used computers at all, and 21% of those who had some computer experience had never used the internet.

Patients' preferences for control over access to EMR data

To examine patients' preferences for sharing EMR data, we first examined whether patients want to share their whole health record, and, second, the patterns of sharing preferences across recipients and record types. The main question is whether participants want to control sharing of their records with recipients, and at what level they desire control (the whole record vs granular control).

Would participants share their whole record?

The first question dealt with in this study is whether patients want to share their whole EMR with potential recipients. Table 3 summarizes the percentage of participants in both patient groups who would unconditionally share all their highly-sensitive or less-sensitive EMR information with various recipients. An examination of the data showed that none of our participants wanted to share all of the information in their EMR with all potential recipients under all circumstances. Furthermore, there was not one potential recipient (eg, primary care physician) with whom all patients wanted to share all of the information in their EMR with unconditionally. This was the case for both groups of participants: those with highly-sensitive health information in their EMR (21 participants) and those without highly-sensitive information (nine participants).

The pattern of percentages in table 3 illustrates several sharing preferences for the whole (or large parts of) EMRs. First, participants do not have the same sharing desires for all recipients; even within medical providers, participants are more likely to want to share their whole medical record with some providers than with others. For example, while three-quarters of participants would share all their health information with primary physicians, less than half would share that information with emergency medical providers, and almost none would share that information with non-treating physicians (NTPs). Second, across the board, participants are less likely to share all their highly-sensitive information than they are to share all their less-sensitive information. For example, while almost all participants would share all their less-sensitive health information with their primary physicians, around one-quarter of those participants would not share all their highly-sensitive information with the same physician. Third, participants with highly-sensitive information in their own medical records are less likely to share all their information with recipients than participants without highly-sensitive information in their records. For example, less than half as many participants with highly-sensitive information would share all their health information with a specialist compared with patients who do not have highly-sensitive information in their records.

A desire for granular control

To understand in more detail patient sharing preferences, we calculated the percentage of items that each participant wanted to share with the various recipients, and we did this separately for highly-sensitive and less-sensitive EMR items. All participants preferred granular control over the sharing of their medical records—that is, all patients wanted to share parts of their record but not other parts with recipients. Furthermore, the sharing preferences are not the same for all participants. The preference for granular sharing can be seen in table 4, which captures each participant's sharing preferences for groups of recipients. The label "coarse" indicates that

Table 3 Percentage of patients who would share all information with a recipient

	Patients with sensitive records (N=21)			Patients without sensitive records (N=9)		
	All items	Less-sensitive items	Highly-sensitive items	All items	Less-sensitive items	Highly-sensitive items
Medical providers						
Primary physicians	76	95	76	78	100	78
Specialists	24	71	24	56	100	56
Emergency medicine	33	71	33	44	89	44
Mental health providers	43	43	43	67	78	67
Nurses	14	43	14	44	67	44
Alternative-medicine	10	24	10	0	22	0
Pharmacists	5	14	5	11	44	11
Home-care rehabilitation	14	33	14	22	56	22
Physician (not treating)	0	10	0	11	22	11
Non-providers						
Health insurance	10	24	10	0	11	0
Family, etc	10	19	10	22	33	22
Researchers	10	10	15	11	11	11
Government agencies	5	10	5	0	11	0
Administration	0	14	0	0	22	0

participants would be willing to provide all medical records with the recipient listed (ie, coarse sharing by recipient) whereas the label "granular" indicates that participants preferred item level sharing of both highly sensitive and less sensitive health information. The label "coarse/granular" indicates that participants would be comfortable with coarse (ie, all or none) sharing of lesssensitive data, but preferred granular (ie, item level) sharing of highly sensitive data.

Differences in sharing patterns

We examined the proportion of information that participants would like to share with recipients and asked whether the sharing patterns differed across recipients, whether they differed based on the sensitivity of the information, and whether they differed for patients with highly-sensitive information in their EMRs compared with those without highly-sensitive information.

We conducted a 2 (patient group)×2 (item sensitivity)×14 (recipient) multivariate analysis of variance (ANOVA) with item sensitivity and recipient as within-subjects factors, and patient group as a between-subjects factor. The dependent variable was the percentage of items a participant reported they would share with each recipient for items in that category (highly sensitive or less sensitive).

Patient groups consisted of two levels: those with highly-sensitive information in their EMR (with sensitive) and those without highly-sensitive information in their EMR (without sensitive).

Table 4 Patient preferences for privacy and sharing control of electronic medical record (EMR) data by recipient group

N (%)	Primary physician	Other medical providers	Non-providers
Patients WITHOUT sensitive health information			
7 (78)	Coarse	Granular	Granular
2 (22)	Coarse/granular	Granular	Granular
Patients WITH sensitive health information			
16 (76)	Coarse	Granular	Granular
4 (19)	Coarse/granular	Granular	Granular
1 (5)	Granular	Granular	Granular

Item sensitivity consisted of two levels: highly sensitive, indicating that the item of information fell into one of the sensitive information categories, and less sensitive, indicating that the item of information was not one identified in the sensitive category.

The recipient factor consisted of 14 levels, for each of the recipients listed in table 1.

The ANOVA revealed three main effects and one interaction, each of which will be discussed in detail. There were no other two-way interactions. The test also showed no three-way interactions.

Patient group

There was a main effect of the between-subjects grouping factor, patient group ($F(1,28)=6.64$, $p=0.016$, $\eta^2=0.192$). Participants with highly-sensitive health information indicated they would share a smaller percentage of their health information (mean=34.8%) than did participants without highly-sensitive information in their EMR (mean=48.6%). This was true across recipients and regardless of item sensitivity, as shown by the lack of an interaction effect with the other factors in the ANOVA.

Item sensitivity and recipients

There was a main effect for each of the two within-subjects factors, item sensitivity ($F(1,28)=67.37$, $p<0.001$, $\eta^2=0.706$), and recipient ($F(13,16)=31.43$, $p<0.01$, $\eta^2=0.962$). However, the main effects for item sensitivity and recipients were qualified by an interaction between these two factors ($F(13,16)=8.43$, $p<0.01$, $\eta^2=0.873$), tempering interpretation. Figure 1 shows the percentage of items shared for highly-sensitive items and for less-sensitive items plotted against recipients (with recipients ordered from those with whom information would be shared most to those with whom information would be shared with least). As can be seen (figure 1), less-sensitive EMR items were more likely to be shared with recipients (mean=54.5%) than were highly-sensitive items (mean=28.8%), accounting for the main effect of item sensitivity. Figure 1 also makes clear the significant difference in sharing across recipients; participants were willing to share significantly more health information with some recipients (eg, primary care physician) than with others (eg, NTP).

Furthermore, figure 1 makes clear that the pattern of differences between sharing of highly-sensitive and sharing of less-

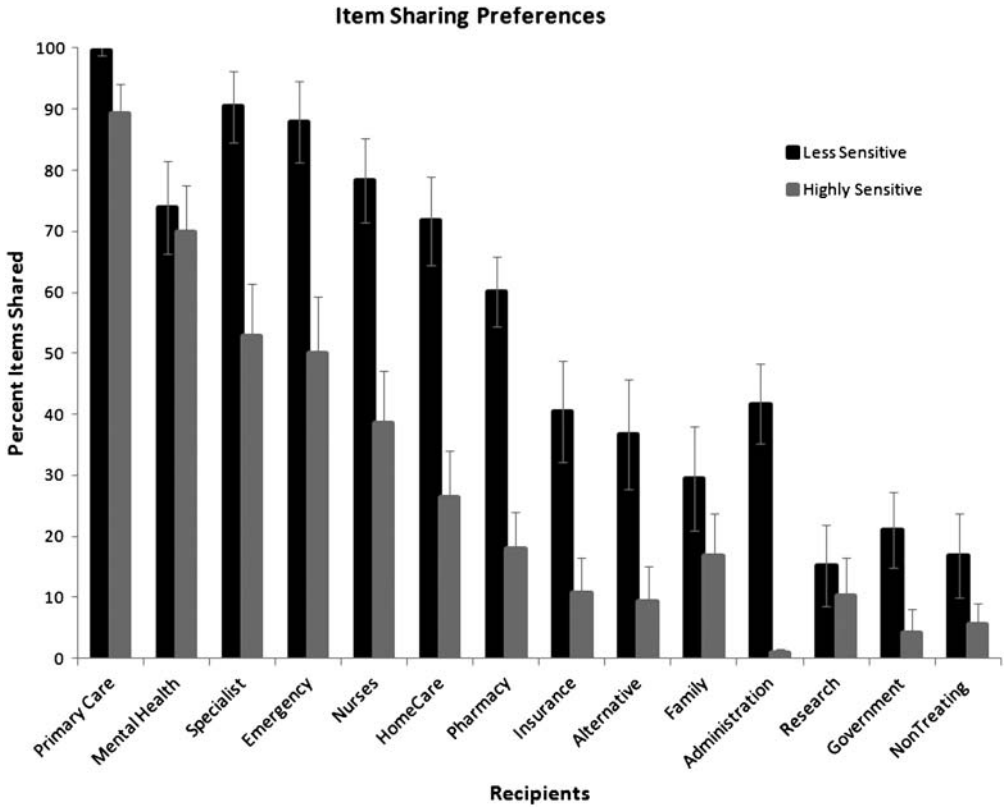

Figure 1 Percentage less-sensitive and highly-sensitive items shared with each recipient across all participants. EMR, electronic medical record.

sensitive items differed across recipients, which gives a visual explanation of the interaction effect. For some recipients the difference is very small, while for others the difference is larger. We conducted a post hoc analysis on the interaction to determine for which recipients sharing patterns were significantly different between highly-sensitive and less-sensitive items, and for which recipients item sharing was not significantly different. We found that the percentage of items shared for highly-sensitive and less-sensitive items differed significantly for all recipients except mental health provider, researcher, and NTP. The difference was marginally significant for family. Participants would share a large percentage of both highly-sensitive and less-sensitive items with their mental health provider. In contrast, participants would by default prefer to share very few items with researchers or NTPs, though participants verbally indicated that they would be willing to share with these recipients if there was a need and they were asked for permission. Many participants indicated the same attitude for family members.

Similar analyses testing differences in sharing preferences between different demographics (gender, age, race, education, health, and income) did not disclose any main effects or interactions. The only exception was an age×recipient interaction ($F(13,16)=3.18$, $p=0.016$, $\eta^2=0.721$). This effect may stem from a difference in sharing preference for home care providers. Those under 46 years of age would share more with home healthcare providers (72% of their information) than those over 46 years (33%). Reasons for this difference could be explored in future research.

DISCUSSION

No participants in this study reported that they would want to share all of the information in their EMR with any recipient unconditionally. This result may be taken as evidence that patients would like to have granular control over the privacy and sharing of information about them in their EMR. This finding is consistent with previous research that investigated patients' desire for individual control over information stored in PHRs,[9] and concluded that 'individuals want control over their information' (p 159). EMR and PHR technologies are considered to be different classes of technology as one contains data collected by healthcare professionals and the other contains information entered by the patient (and, in some cases *also* data shared by healthcare providers), but it is likely that this distinction will (and should) fade as pieces of health information from a variety of sources are adopted and used throughout the healthcare ecosystem.

Historically, granular control over privacy and sharing of health information has existed, even if that control has been applied by different means (eg, by avoiding a regular physician for certain conditions[10]). For a simple example of the historical ability of patients to restrict the sharing of their personal health information consider the following situation: a patient wishes to limit the information her primary care physician receives about her mental health status. She may choose to visit a mental health provider who practices outside the health system where she sees her primary care provider. Under the current system, records that are collected about her at her mental health provider's office must be purposefully transmitted, either by paper or electronically, to other providers including the primary care provider. However, if the patient prefers to limit the sharing of this information the patient may simply choose not to let the primary care physician know that she is receiving mental healthcare and may ask for no records to be shared. Thus, the overall finding that patients want to

maintain the level of privacy and control over the destiny of their health information is not surprising as it simply reflects their current rights and abilities.

Sharing by recipient

In addition to understanding patients' overall preferences for sharing EMR data, we were also interested to learn how preferences varied across potential recipients. Our primary goal was to understand patients' preferences for sharing EMR data with medical providers, which we consider in the following section. We have examined the results related to primary physicians separately because patients' preference for sharing with their primary physician was qualitatively distinct from sharing with other medical providers.

Sharing with primary physician

Most patients reported that they would want to share all of the less-sensitive information in their EMR with their primary physician. This preferred sharing pattern represented the highest level of sharing across recipients. However, even in this case, five participants whose records contained sensitive information and two participant whose records did not contain sensitive information reported that they would not want even their primary care physician to have unconditional access to all of the sensitive data elements in their EMR. For example, one participant reported that she would not share substance abuse, domestic violence, genetic or reproductive health information (P5); one would not share genetic, reproductive health or sexual health information (P12); one would not want to share domestic violence or reproductive health information (P15); one would not share mental health information, domestic violence, reproductive or sexual information (P30); and one participant reported that she would not share genetic information (P18).

The reasons for specific privacy preferences varied across participants. For example, P18 argued that medical providers should not have unrestricted access to genetic information because this contained information about 'potential that may or may not bare'. In other words, she was concerned about consequences of being genetically predisposed to certain conditions (she specifically mentioned mental health conditions) and how this predisposition might result in provider bias. This particular participant generally expressed very liberal sharing preferences (ie, thought medical providers should have access to most of her information) across medical providers, but made a distinction between information about something that 'has happened' versus 'could happen' and felt that it would be 'tricky' to share information about what 'could happen'. Another participant reported concerns about potential provider bias due to information contained in a record, 'what if they knew I used to abuse drugs or alcohol? They might not treat me the same' (P20). Many participants did not want to share private information if it was not specifically needed for their medical care. For example, one participant reported that she would not want to share information about a suicide attempt when she was very young, saying if she is seen for 'bronchitis or something like that. Why does he (medical provider) need to know that?' (P30). Unless the information specifically aided her health in some way, it was not information she wanted to share even with a primary physician.

Sharing with all other medical providers

Table 3 provides a list of medical providers other than primary physicians. This includes specialists, emergency medical providers, mental health providers, nurses, alternative-medicine providers, home-care or rehabilitation therapists, and NTPs.

No participants we interviewed wanted to unconditionally share all of the information in their EMR with medical providers who were not their primary physician. Participants' desire to share sensitive information with these medical providers is even more guarded than preferences for sharing with a primary care physician.

The order of sharing preferences is reflected in table 3 where recipients are ordered by descending percentage of participants who would want to share all information with that recipient, and in figure 1, which shows the percentage of information shared with each recipient. More participants would share all their records with specialists than others in the list, followed by emergency medicine providers, mental health providers, nurses, and so on. Patients are less likely to share all their information with specialists than with primary physicians. Most participants (80% of all participants) would share all their less-sensitive health information with specialists, and only around one-third of participants (30%) would share all their sensitive information with that provider. This can be contrasted with the greater openness shown to sharing with primary physicians. Perhaps not surprisingly, most participants preferred not to share all medical records with doctors who were not currently treating them. Similar to results related to preferences for sharing with primary physicians, participants reported that sharing with other medical providers should be specifically related to the present health condition. For example, one participant commented with respect to a pharmacist, 'just because they're giving me medication, they don't need to know that I had herpes or whatever health situation. They don't need to know that'.

The results related to the pattern of sharing preferences across recipients will be helpful to designers who would like to understand overall patient preferences for sharing of EMR data. One specific design implication that may be drawn from these data is in the need to set default privacy settings for EMRs. Default privacy settings are considered very important in the design of information sharing interfaces because users rarely change default settings.[11] Thus, by understanding patients' overall preferences for sharing, designers can create sharing/privacy default settings that will reflect patients' desires. In future research and in partnership with designers, we hope to generate such default EMR sharing settings and test these with patients.

Sharing with non-provider recipients

In addition to understanding patients' preferences for sharing EMR data with recipients who at present may potentially access EMR data, we were also interested in understanding patients' preferences for sharing EMR data with recipients who do not currently have access. To understand these preferences we examined patient preferences for sharing with health insurance companies, researchers, government agencies, administration, and family and friends. Patients were far less likely to indicate they would share their whole medical record with non-providers than with health providers (table 3), and they indicated they would share fewer items of information with recipients in this group (figure 1). In most cases, participants said they would want to be asked before providing EMR access to recipients in this group. In the case of health insurance companies, patients' preferences reflect their feeling that there is less choice about what to share.

Summary: sharing across recipients

When considered within the context of other research on privacy and sharing preferences, the finding that patients wanted to share different information with different recipients is not surprising. Across a variety of settings, people prefer to share information differentially depending on the recipient or recipient group. For example, when giving details of location, people prefer to share the information *at different levels of granularity* (eg, exact address vs city, state) depending on the recipient (eg, significant other vs coworker[12]). In the home, people's sharing preferences for music, photos, and other files varied by recipient and were influenced by multiple factors such as physical presence and time of day of access.[13] Similarly, we found that patients wish to share their health information differentially depending on the recipient of the information and other contextual factors. Technical work[14] and policy work[15] enabling fine-grained access to electronic health information is already underway that will facilitate access to elements differentially by provider types.

Differences in preferences of patients whose records contain sensitive data

Across medical providers, sharing preferences are strikingly different for participants who have sensitive health information compared with those who do not. The proportion of information shared by patients with sensitive health information in their own records is significantly less than for patients without such information. For example, for sharing with specialists, around two-thirds of participants in the sensitive health information group prefer to share all less-sensitive health information, and around one-quarter of those patients would share all their sensitive information. In contrast, participants not in the sensitive information category were unanimous about sharing all less-sensitive information with specialists, and more than half would share all their sensitive information. There are many potential explanations for this difference. First, patients with highly-sensitive information in their records might have had a previous experience where they did not want this information shared with a provider or other recipient. As in other areas of privacy decision-making (eg, setting privacy controls in online social networks), it is probably difficult for patients to explain why they want information to remain private (not shared with a specific recipient). Second, the difference between patients with and without sensitive information may be a reflection of the tendency for the participants in our study who had sensitive health information to rely on a primary physician for almost all of their healthcare needs, and thus other healthcare providers did not need to have full access to all EMR data.

Preferences of all patients about sensitive elements

Whether participants were patients with highly-sensitive health information in their records or not, they were more likely to share less-sensitive health information items with recipients than highly-sensitive health information (figure 1). This was true for almost all recipients with the exception of mental health providers, researchers and NTPs, as indicated previously. In the case of mental health providers it may be that patients were likely to share a large part of their sensitive information (as well as their less-sensitive information) because sensitive issues may be particularly relevant to mental healthcare. For researchers and NTPs, the tendency was for no information to be shared (sensitive or otherwise), unless there was a need and patients gave permission for that specific case. However, the distinction made by NCVHS for items that are considered 'sensitive' may not be sufficient as we found that preferences for sharing even less-sensitive items varied across participants. This finding indicates that what one patient considers less sensitive may be considered highly sensitive by another. Once again, this finding is in line with previous research on the human factors of privacy: privacy preferences and perceptions of sensitivity vary from person to person. For example, across a variety of information types some clusters of information were treated similarly by participants, but even these clusters were highly variable between people,[16] and people's perceptions of which data from the home environment were considered sensitive varied, resulting in different ideal policies across households.[13]

These differences in sharing preferences for a particular type of information in the EMR are a fundamental indication of the need to provide patients with granular privacy control not only over information that may be considered sensitive by a governing body, but over all information in an EMR, thus ensuring that diverse patient perceptions about item sensitivity are respected. This is essential so that individual patients can maintain privacy control over what *they* consider to be sensitive.

Conditional sharing

None of the patients we interviewed stated that physicians or other healthcare providers should be absolutely *prohibited* from seeing information in their EMR under all conditions. Instead, for some recipients, while participants did not indicate they would share information unconditionally, they reported that they would give access if needed (ie, conditional sharing). For example, most participants said they would not share any records unconditionally with NTPs, but that they would share parts of their health information if there was a demonstrated need. Participants also indicated that they would like to give temporary access to certain recipients based on need and for that need only. For example, most participants did not want to give researchers access to their whole EMR, but just the part of the EMR that the researcher needed when asked (they would give permission for a limited time). Likewise, they might provide limited, temporary access to government agencies or various physicians as needed.

Another indication of a preference for temporary, granular access is that patients would like doctors who are no longer treating them no longer to have access to their records.

In general, patients indicated they would share information if it is used for their health benefit but otherwise prefer it to remain private, which is a common finding across privacy studies.[17]

Limitations

One significant limitation of this study is that we did not use personalized patient EMR data during the card-sort task. Participants were given veridical examples of information that could exist in their EMR, but their data were not presented to them. A common finding from privacy literature in other domains[18] is that de-contextualized sharing preferences often do not match actual sharing behavior. It is unclear whether this mismatch is due to participants' inability to control sharing, lack of understanding about what is being shared and with whom, or whether in situ preferences differ from a priori preferences. Whatever the reason, the limitation to this study is clear: if participants had examined their own records they might have identified items they did not recall or know about

previously, and this experience might have influenced their sharing preferences. In future studies, as well as in the design of privacy-enhanced EMRs it will be important for patients to see their own EMR data as they make privacy and sharing decisions.

CONCLUSION

Our work demonstrates that patients want granular privacy control over sharing of information of their EMR data. We found that none of our participants wanted to share all of the information in their EMR with all potential recipients under all circumstances. Instead, our study showed that for privacy to have meaning, patient-directed granular control over EMR data is necessary.

Acknowledgments We thank the anonymous reviewers for their insightful suggestions. We would also like to thank the William Tierney, Eric Meslin, Sheri Alpert, Peter Schwartz, Aaron Carroll, Jere Odell, Mike Barnes, Jon Duke, Jeff Friedlin, Doug Martin, Michele Degges, Morgan Soladine, Denise Anthony, Kay Connelly, Crystal Boston, Nathan Mihalik, Brenda Hudson, Jane Anne French, Patrick McGuire, Laura Yorger, Bedellion Armstrong, Kelli Givens, Genesis Thomas, Jennifer Hutchenson, Allison Stieneker and Marc Overhage.

Contributors KC is responsible for the conceptualization and initial design of this work. RH helped refine the design, and led data acquisition and data analysis. Both authors participated in the interpretation of the data and the writing and editing of the manuscript.

Funding This work was supported in part by cooperative agreement award number 90HT0054/01, from the Office of the National Coordinator, Department of Health and Human Services for the State Health Information Exchange - Cooperative Agreement Program with the Indiana Health Information Technology, Inc., the Center for Law, Ethics and Applied Research in Health Information and the School of Informatics and Computing at Indiana University.

Competing interests None.

Provenance and peer review Not commissioned; externally peer reviewed.

REFERENCES

1. **President's Council of Advisors on Science and Technology.** Realizing the Full Potential of Helath Informaiton Technology to Improve Healthcare for Americans: The Path Forward. 2010. Retrieved from http://www.whitehouse.gov/sites/default/files/microsites/ostp/pcast-health-it-report.pdf
2. **Boonstra A,** Broekhuis M. Barriers to the acceptance of electronic medical records by physicians from systematic review to taxonomy and interventions. *BMC Health Serv Res* 2010;**20**.
3. **Barrows RC,** Clayton PD. Privacy, Confidentiality, and Electronic Medical Records. *J Am Med Inform Assoc* 1996;**3**:139–48.
4. **Sparck-Jones K**. Privacy: what's different now? *Interdiscip Sci Rev* 2003;**28**:287–92.
5. **Kuperman GJ.** Health-information exchange: why are we doing it, and what are we doing? *J Am Med Inform Assoc* 2011;**18**:678–82.
6. **Kaelber DC,** Jha AK, Johnston D, *et al*. A research agenda for personal health records (PHRs). *J Am Med Inform Assoc* 2008;**15**:729–36.
7. **Office of the National Coordinator for Health Information Technology, & U.S. Department of Health and Human Services**. Nationwide Privacy and Security Framework For Electronic Exchange of Individually Identifiable Health Information. 2008. Retrieved from http://healthit.hhs.gov/portal/server.pt/community/healthit_hhs_gov__privacy___security_framework/1173
8. **Carr JM.** National Committee on Vital and Health Statistics Recommendations Regarding Sensitive Health Information. 2010. Retrieved from http://www.ncvhs.hhs.gov/101110lt.pdf
9. **Civan A,** Skeels MM, Stolyar A, *et al*. Personal health information management: consumers' perspectives. *AMIA Annual Symposium Proceedings* 2006:156–60.
10. **Bishop L,** Holmes BJ, Kelley C. *National consumer health privacy survey*. California HealthCare Foundation, 2005.
11. **Gross R,** Acquisti A. *Information revelation and privacy in online social networks*. Paper presented at the Proceedings of the 2005 ACM workshop on Privacy in the electronic society, 2005.
12. **Consolvo S,** Smith IE, Matthews T, *et al*. *Location disclosure to social relations: Why, when, & what people want to share*. Paper presented at the Proceedings of the SIGCHI conference on Human factors in computing systems, 2005.
13. **Mazurek ML,** Arsenault JP, Bresee J, *et al*. *Access Control for Home Data Sharing: Attitudes, Needs and Practices*. Paper presented at the Proceedings of the 28th international conference on Human factors in computing systems, 2010.
14. **Sujansky WV,** Faus SA, Stone E, *et al*. A method to implement fine-grained access control for personal health records through standard relational database queries. *J Biomed Inform* 2010;**43**(5, Supplement):S46–50.
15. **Trojer T,** Katt B, Schabetsberger T, *et al*. *Considering privacy and effectiveness of authorization policies for shared electronic health records*. Paper presented at the Proceedings of the 2nd ACM SIGHIT International Health Informatics Symposium, 2012.
16. **Olson JS,** Grudin J, Horvitz E. A study of preferences for sharing and privacy. *CHI '05 extended abstracts on Human factors in computing systems*, 2005.
17. **Caine KE,** Fisk AD, Rogers WA. Benefits and privacy concerns of a home equipped with a visual sensing system: a perspective from older adults. *Proc Hum Factors Ergon Soc Annu Meeting* 2006;**50**:180–4.
18. **Spiekermann S,** Grossklags J, Berendt B. *Eprivacy in 2nd generation e-commerce: Privacy preferences versus actual behavior*. Paper presented at the Proceedings of the 3rd ACM conference on Electronic Commerce, 2001.