Designing a Patient-Centered User Interface for Access Decisions about EHR Data: Implications from Patient Interviews

Kelly Caine, Ph.D.[1,2,3], Spencer Kohn, B.A.[1], Carrie Lawrence, Ph.D.[2,4], Rima Hanania, Ph.D.[2,5], Eric M. Meslin, Ph.D.[2,6], and William M. Tierney, M.D.[3,7]

[1]Clemson University School of Computing, Clemson, SC, USA; [2]Center for Law, Ethics and Applied Research in Health Information, Bloomington, IN, USA; [3]Indiana University, Bloomington, IN, USA; [4]Indiana State University, Indianapolis, IN, USA; [5]Department of Psychological and Brain Sciences, Indiana University, Bloomington, IN, USA; [6]Center for Bioethics, Indiana University, Indianapolis, IN, USA; [7]Regenstrief Institute, Inc, Indianapolis, IN, USA.

BACKGROUND: Electronic health records change the landscape of patient data sharing and privacy by increasing the amount of information collected and stored and the number of potential recipients. Patients desire granular control over who receives what information in their electronic health record (EHR), but there are no current patient interfaces that allow them to record their preferences for EHR access.

OBJECTIVE: Our aim was to derive the user needs of patients regarding the design of a user interface that records patients' individual choices about who can access data in their EHRs.

DESIGN: We used semi-structured interviews.

SETTING: The study was conducted in Central Indiana.

PARTICIPANTS: Thirty patients with data stored in an EHR, the majority of whom (70 %) had highly sensitive health EHR data, were included in the study.

APPROACH: We conducted a thematic and quantitative analysis of transcribed interview data.

KEY RESULTS: Patients rarely knew what data were in their EHRs, but would have liked to know. They also wanted to be able to control who could access what information in their EHR and wanted to be notified when their data we re accessed.

CONCLUSIONS: We derived six implications for the design of a patient-centered tool to allow individual choice in the disclosure of EHR: easy patient access to their EHRs; an overview of current EHR sharing permissions; granular, hierarchical control over EHR access; EHR access controls based on dates; contextual privacy controls; and notification when their EHRs are accessed.

KEY WORDS: privacy; fair information practice; electronic health records; patient preferences; human factors.
J Gen Intern Med 30(Suppl 1):S7–16
DOI: 10.1007/s11606-014-3049-9

INTRODUCTION

As a nation, we are making progress toward the goal of seamless, user-transparent, cross-organizational health data exchange.[1,2] In 2010, the President's Council of Advisors on Science and Technology asserted that "The overarching goal is to have a national health information technology (IT) ecosystem in which every consumer, doctor, researcher, and institution has appropriate access to the information they need, and in which these groups are served by a vibrant market of innovators."[3] One technology that has the potential to improve care by providing an integrated view of relevant patient information is the Electronic Health Record (EHR).[4]

EHRs collect and disperse patient health information to a variety of recipients beyond the provider who collected it. Recipients of data contained in integrated EHRs range from providers who are actively treating a patient, to non-provider members of the health care industry, such as insurance companies or government agencies. Such data sharing has the potential to improve quality of health care by reducing errors and lowering costs.[5] However, along with these positive effects, data sharing also has the potential to vastly decrease patient privacy, and in turn affect patients' openness and relationships with their health care providers (i.e., be a "double edged sword.")[6]

Previous research suggests that patients who are concerned about the privacy of their health information engage in risky health behaviors such as being less likely to seek care, refusing to discuss problems openly with their providers, delaying care, and even lying to providers (e.g., [6,7]; also see[8] for a thorough review). Thus, realizing the potential of Health IT to positively transform health care depends on whether or not new technologies respect patients' privacy preferences.

In 2010, the Office of the National Coordinator for Health Information Technology (ONC) published a Health Information Exchange Challenge Grant Program that included a call for proposals for "enabling enhanced query for patient care." One goal was to develop a usable, web-based user interface (UI) for patients to express their preferences about who could access what data in their EHRs. We have previously described an ethics framework to aid development of a patient control

Electronic supplementary material *The online version of this article (doi:10.1007/s11606-014-3049-9) contains supplementary material, which is available to authorized users.*

Published online December 6, 2014

tool,[9] which is extended in another paper in this JGIM Supplement,[10] and how we developed and implemented the revisions to Careweb, a local utility for viewing EHRs.[11] In this article, we continue to further privacy-enhanced EHR research by deriving implications for the design of a user-friendly web-based UI from interviews with patients about their needs and desires for controlling who can access personal information in their EHRs. Because we are interested in learning directly from patients what is important to them and why, we used a qualitative approach.[12]

METHODS

This study is part of a larger project investigating patient sharing and access preferences to electronic health records. This portion of the study is the interview, which focused on understanding patient preferences for, attitudes about, and strategies for managing the privacy of a patient's EHR and the design implications thereof. In this section, we provide the key items requested by Tong et al.[13]

Recruitment and Participants

The 30 adult participants in this study are the same as those reported in Caine and Hanania.[14] Participants were invited to participate if they fulfilled the following criteria: currently receiving health care in central Indiana and having active health records in the Indiana Health Information Exchange.[15] We purposefully oversampled patients whose EHR contained highly sensitive health information as defined by the National Committee on Vital and Health Statistics (NCVHS);[16] specifically, one of the following: domestic violence, genetic information, mental health information, reproductive/sexual health, and substance abuse. Patients whose records contained sensitive information were identified by the Indiana Clinical and Translational Sciences Institute (CTSI) for recruitment. No detailed information from the patients' EHR was accessed by study staff.

Patients were either (1) approached by recruiters during outpatient appointments, told about the study, and invited to participate; or (2) recruited from a volunteer recruitment registry for residents in Central Indiana called INResearch.[17] Patients who expressed interest were contacted for scheduling. Four additional participants were recruited through flyers posted on the Indiana University campus. The Institutional Review Board at Indiana University and the Indiana Network for Patient Care[15] Management Committee approved this study, and each participant provided written informed consent.

Procedure

The procedure was identical for all 30 participants: after filling out paper questionnaires, participants completed two information-architecture card-sorting tasks (see [18]), a semi-structured interview, and a sharing-preferences card-sorting task (see [14]). This paper reports on the results of the semi-structured interview, as well as demographics from relevant questionnaires.

Interview Guide

We created a semi-structured script to elicit information from patients about their understanding of their current medical records, what methods they were aware of to view and exert control over the sharing of their health information, aspirations for future data sharing capabilities, as well as specific privacy concerns related to the sharing of health information.

While we employed guided questioning to facilitate consistent information elicitation across participants, the semi-structured interview format allowed the interviewer flexibility to follow up on themes we had not identified prior to creating the interview guide. The interview guide was pilot tested with three participants prior to beginning data collection to ensure that it was comprehensible and comprehensive. The interview script is available as an online Appendix.

Data Capture and Transcription

Interviews were video-recorded and audio-recorded and transcribed verbatim by a professional transcriptionist prior to the analyses.

Analysis

In preparation for analysis, all transcripts were entered into MAXQDA,[19] a computer program for qualitative data analysis. Following initial familiarization with the data, we performed a thematic analysis. We developed an initial coding scheme and performed indexing though constant comparison within and between interviews. Then, an independent meta-analysis was conducted using the coding scheme to synthesize the initial findings.[20] Transcripts were initially coded by a researcher (CL) with expertise in qualitative inquiry and health behavior, then categories were developed and refined based on previously reported quantitative data and in discussion with the project team. Two investigators (CL & SK) then independently coded all quotations from participants. Any disagreements in coding were settled by a third researcher (KC).

RESULTS

Demographics

The 30 participants in this study were the same as reported in Caine and Hanania.[14] Enrolled patients were 73 % women, 30 % minority (African-American or Multiracial), and had a mean age of 46±12 (SD) years. Patients ranged in educational

attainment between less than high school to having graduated from college; represented a large range in household income, from those earning less than $5,000 per year to over $100,000 per year; represented a large range of self-reported health statuses, and a range of computer and internet experience. Seventy percent of participants had highly sensitive information in one or more of the five categories considered to be highly sensitive by the National Committee on Vital and Health Statistics.[16]

Interviews

All participants completed the interview (see Table 1 for summary). Few patients (10 %) reported that they could currently access their EHR, and half had little to no idea what might be contained in their EHR. Participants unanimously (100 %) reported that they would like access to the information contained in their EHR. For example:

> Ideally, I'd like to have the same access to see what the doctors see. You know, and to see all the history and results, even the notes they've written. (P4)

None of the patients knew precisely who could view information about them via an EHR. All participants (100 %) reported that they would like to know and be able to control what entities accessed information in their EHR:

> In a nirvana situation, I would have control over what he would look at, whether, and ask why would he want to look at that. (P15)
> It's my body, that's my information and how you handle it, it should be decided by me… Your medical record is you, I want to be the curator. I want to be the person who decides how it's maintained, what's put in it, what's preserved and how it's shared. (P25)

Reasons for wanting control over access varied. For example, one participant felt information was too private and personal to share:

> You're not wanting everyone to know your sexual history even if it isn't bad. That's private, personal stuff. You aren't going to want everybody to have access to that. (P20)

Another participant did not express *why* she would want control, but did say there were things about her past medical encounters that she:

> don't want him [physician] to know. (P12)

All participants (100 %) reported that they would like to be notified when their EHR was accessed so they would know what information was viewed and by whom. For example:

> I'd like to be notified anytime anybody accesses my medical records. Even if it's my primary care physician… I'd either be notified through email or whenever you log on…. When you log on, you should be able to see a list of everybody who's accessed your file. (P23)
> If it's electronic, you'd be notified if they're trying to access something that's more confidential. (P5).

Other participants mentioned that this type of notification would help them maintain trust with their provider:

> A good system would be able to track who accesses it and determine whether or not they had a reason to do so. (P19)

Participants described three distinct methods for how they would like to manage access control of their EHR: 1) granting permission, 2) blocking/restricting certain information, and 3) restricting access based on the time period during which it was collected. The majority of participants (93 %) wanted to be able to grant permission for recipients to view EHR data:

> I would like there to be a permission system that nobody else has access unless they are an authorized

Table 1. Patient Knowledge, Access and Preferences for EHRs

Overall (N=30) (%)	
Know what is in EHR	
Yes[*]	3 (10)
Somewhat	12 (40)
No	15 (50)
Have access to information in EHR	
Yes	3 (10)
No	27 (90)
Believes they knows who can view EHR	
Yes[†]	1 (3)
No	29 (97)
Desire access to one's Medical Record	
Yes	30 (100)
No[‡]	0 (0)
Desire control over access to health information	
Yes	30 (100)
No	0 (0)
Would like notification when EHR is accessed	
Yes	24 (80)
No	6 (20)
Methods of access control[§]	
Granting permission	28 (93)
Restricting/blocking specific information	9 (30)
Time limits/temporal control	6 (20)
Access on "need to know" basis	
Spontaneously mentioned	25 (83)
Not mentioned	5 (17)
Stated that they do not know what doctors need to access	
Spontaneously mentioned	6 (20)
Not mentioned	24 (80)

[*] *Same three participants who reported they had access to their EHR*
[†] *Patient stated that only his primary doctor could view his EHR*
[‡] *Three participants mentioned they would not want online access to EHR because of privacy/security concerns*
[§] *Does not sum to 100 % because participants could mention multiple methods*

> health care provider or you've granted them access.(P17)
> There are certain things that I don't want just anybody to have access to unless I grant it. Just because North Carolina's doctor would want that information doesn't necessarily mean that I would want North Carolina's doctor to have that information. (P30)

One participant described how she would like to be able to grant permission before information was added to her EHR:

> Let's talk about my care… I think the doctors too have to use the patient as his first resource… If there's something that needs to be put on the record, doctor says to the patient, 'Okay, we need to update your record. Do I have your permission to add this information to your master record, to your medical file, your medical history?' (P25)

A minority of participants (30 %) mentioned a desire to be able to block or restrict access to specific information by recipient.

> Then, you can check that select all button when you're not wanting to see it, to block them from having any new access. (P27)

A small minority of participants (20 %) described a desire for temporal control where they could restrict information based on the time period during which data were collected. For example:

> It goes back to the relevance of it… What if that was when I was fifteen? … why does he need to know that, especially if it's something that has never come up before. (P30)
> I don't really think they necessarily have to have that in order to do their job… To schedule or bill something, I don't think they need to know what's happened in the past. (P6)

Other participants focused their time-based comments on how long providers should have access to information after a care event:

> See it all but then turn it off later when they're no longer your doctor. (P27)

While we did not have a question in our interview script that specifically asked about "need to know" or relevance of EHR data on care, this topic emerged as a dominant theme throughout the interviews. A majority of participants (83 %) spontaneously mentioned that access to EHR data about them should be accessed only on a "need to know" basis. That is, recipients should only access EHR data when that specific information was needed for a particular care event. For example:

> A nurse practitioner that I'm going in to see about migraine headaches doesn't need to know if I had an STD 3 or 4 years ago. Doesn't need to know sexual orientation. Doesn't need to know I had a colonoscopy a couple of years ago. I'm there to see her about migraines. She just needs to be able to access information pertinent to my migraine history. (P23)
> This is irrelevant information to them, I think…Yes. I would say, that's my personality. They don't get any information they don't need. (P13)
> Why they were having access to it when I am getting treated for a broken leg or whatever it might be. If I am in the hospital for an appendectomy why are they getting this kind of stuff? So I really wouldn't want them to have it because I don't think they need to have it. So I'd feel that is was a kind of violation. That is too strong a word but I don't know what… I just don't know why they would need to see any deeper than this. (P4)
> Is there anything that lab technician has to know?… Let's say you had something they needed to know. Then they would have limited access to that health information, but they wouldn't have to see everything. (P18)

Some participants (20 %) felt that they might not always know what "needs" to be accessed:

> I'm not in a position to determine whether or not, what information is or is not exactly medically appropriate for them to see. (P17)
> …if it's up to the individual to limit access to different doctors, as I said, the individual is not a doctor. They don't know what information the doctor might need. (P23)

One participant suggested that the primary care physician should determine what other providers "need to know":

> [if a specialist needs information] They have to see my [primary] doctor (P14)

And another suggested a health "team" could determine under what conditions to grant access:

> There should be like a team that's in the medical records that's responsible for granting the access for emergency situations… they would have to say what they're needing it for and determine if they would need just this particular area or if they need everything.

DISCUSSION

Our results, when viewed in combination with the ONC for Health Information Technology (HIT)'s privacy and security framework—eight principles that serve as a data collection framework for the protection of consumer privacy[21]—suggest six implications for the design of a patient-centered[22] tool allowing patients to control disclosure of their EHR data. These six design implications are: 1) easy patient access to their EHR data, 2) reports of what is currently shared with whom, 3) granular, hierarchical control, 4) time-based controls, 5) contextual privacy controls, and 6) access notification.

Easy Patient Access to EHR Data

Individual access, or ensuring that people have access to data collected about them, is a core principle of fair information practice,[23] and is a requirement for patients to be able to effectively control the privacy of their EHR data. Furthermore, patient access to one's EHR data may improve the patient–provider relationship and engage patients in their own care.[24,25] Despite these benefits, only one-third of US physicians think patients should have full access to their EHR information.[26]

Fifty percent of patients in our study reported that they had no idea what was stored in their medical record and 90 % reported that they did not have access to their EHR. When patients gain access to their entire health record, they want to continue to access it, even though their privacy concerns about the data shared online increase.[27] To be able to make informed decisions about sharing EHR data and personal privacy, patients must first be able to see what data about them are stored. Ideally, patients should be able to access their information in a variety of ways, including online, in the provider's office and via paper letters and reports.

Summary of What is Currently Shared With Whom

Another core principle of the ONC's privacy framework is "openness and transparency." No patients in our study expressed knowledge of the reality of how widely their health information is actually shared (e.g.,[28]; see[29] for a visualization). Indeed, EHR information can be shared quite widely. For example, Indiana has a health information exchange, the INPC[15], which contains updated information from more than 90 Indiana hospitals and their affiliated outpatient practices. Physicians and other health care providers from these hospitals have access to patient data from all INPC hospitals. The INPC maintains a log of who accesses each patient's record, and when, but does not record what information is displayed to users.

Therefore, a critical element of a user interface for patient control of EHR data is an overview of how current EHR data are shared. We propose a dashboard (see Fig. 1) where patients can quickly gain an overall understanding of what categories of information in their EHR are shared with whom.

Each category of health information is expressed as a column along the semi-circle and each recipient group is represented as a row. In this concept, existing sharing settings are reflected via colored blocks: a colored block at the intersection of the Mental Health column and the Specialists row indicates that health specialists currently have access to Mental Health information. Health care providers are positioned closer to the center, while non-providers (e.g., Government) are positioned on the outskirts of the semi-circle. Overall, the concept is meant to provide a fast and intuitive glimpse of how a patient's data are currently shared.

Provide Granular, Hierarchical Control

Similar to previous research (e.g.,[30,31]), participants in our study expressed a wide variety of preferences for what information they would like to share with whom,[14] and how they would like to achieve this control (see Table 1). While all participants wanted to control who could view information contained in their EHRs at some level of granularity, the level at which participants wanted to exert regular control varied. Furthermore, there were differences in how users thought they could most effectively achieve this control. For example, some conceptualized allowing access to information (similar to findings reported in[30] and[32]), while others talked about restricting access to information.

One user interface (UI) approach for supporting diverse preferences at a variety of levels of granularity simultaneously is to provide hierarchical control. Hierarchical control allows patients to select the level of granularity at which they make decisions and also allows patients to both allow and restrict access. For example, for those patients who prefer to share their entire EHR with all providers, they can affect this at a very high level in the UI. On the other hand, patients who would like to share all but selected sensitive categories of information with all providers can move down a level in the hierarchy. Finally, patients who would like to exclude one test from being shared with a provider or providers, or vice versa, could access this level of detail to make this choice.

We propose a system where users can drag-and-drop a category of health information into a specific recipient (e.g., primary care physician) or a set of recipients (see Fig. 2). Patients desiring further customizability can venture into the drop-down menu of a health data category and limit which recipients would receive specific pieces of information.

A hierarchically based user interface for patient-directed control over access to EHR information with drag-and-drop functionality is shown in Fig. 2. Groups of health information are in the left column, and groups of recipients are on the right.

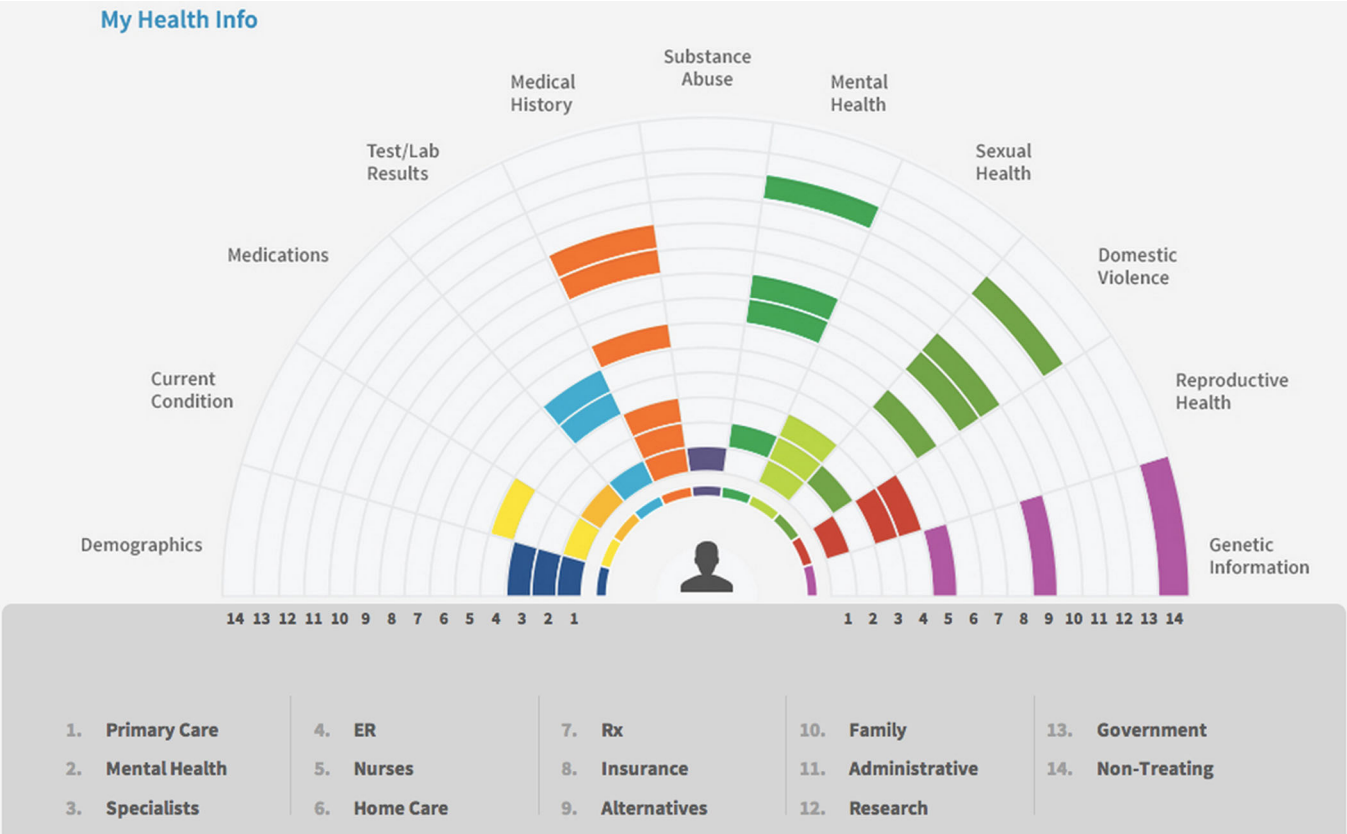

Figure 1. Overview dashboard concept. Columns represent health information categories, while rows represent recipients. Current sharing settings are represented by colored blocks

Access is granted or rescinded by dragging a health information group such as Test/Lab results into a recipient group such as Primary Care. Individual elements (e.g., a specific lab result) are accessed by clicking on the category level and can be dragged in or out, thus granting or restricting just at the category level. Provider groups are created by dragging provider circles together. The colored dots within each provider circle represent the information categories currently shared with each provider group.

Time-Based Controls

In addition to expressing the desire to control what elements of their EHR could be shared with whom, some patients expressed the desire to restrict information based on when it was collected. We propose including a time-based control element where patients can restrict certain information based on the time it was collected (see Fig. 3). From a technical perspective, this may be difficult to implement, as discussed in detail in another article in this *JGIM* supplement.[11] Access to information recorded on a particular date can easily be restricted, but redacting information in free-text notes and reports concerning past events requires complex natural language processing.

Contextual Privacy Controls

In addition to providing patients control through a hierarchical user interface, and offering them the ability to set limits to information access based on the time it was collected, we also suggest that the user interface should allow patients to make sharing and privacy decisions in context, i.e., during a medical encounter, in the context of the appointment, or in the context of the health information display itself while viewing their EHR. Privacy decisions are difficult across domains, especially when de-contextualized, and may not match actual privacy behaviors.[33] Providing contextual privacy controls would increase the likelihood that privacy choices match with privacy preferences.

We propose a concept interface that enables contextual control by allowing patients to set privacy levels in the context of viewing events within an EHR (see Fig. 4). This user interface is complementary to the other two control concepts in that it exists within the EHR interface itself, rather than as a separate piece.

Access Notification

A majority of study patients (80 %) would like to know when their EHR information had been accessed and by whom, but

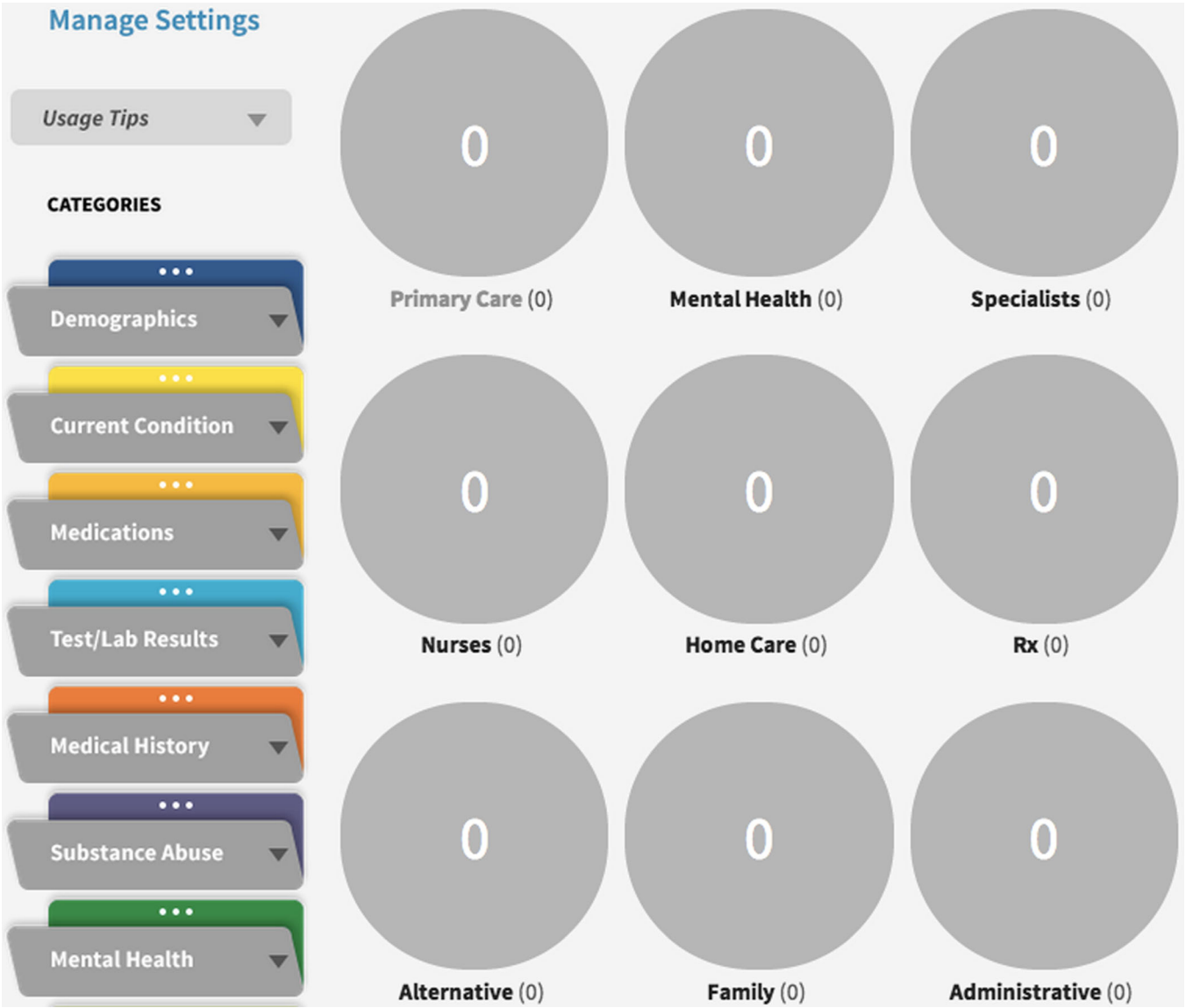

Figure 2. A hierarchal drag-and-drop user interface concept for patient-directed control over access to EHR information. Categories of health data are contained in the column on the left. Drop down functionality enables granular access to individual data. Groups of potential recipients are represented in the circles

varied in their desires for frequency of notification. Some patients wanted to be notified about every EHR access, while others wanted to know only when sensitive or confidential information was viewed. Importantly, patients suggested that having this kind of notification would enhance their trust in their provider and in the health system, which is notable, since previous research has pointed to the importance of patient trust in their care team on willingness to share personal health information (e.g.,[31]).

Figure 3. A menu bar concept clearly displaying the time limits option

Access notification is also related to the ONC's privacy framework principles of "safeguards" and "accountability."[21] Safeguards refer, in part, to the necessity of preventing unauthorized access to EHR data, while accountability refers to the active monitoring that should take place to ensure that there is no unauthorized access. Patients can be part of the safeguard and accountability system (though this is not a substitute for other policies and protections) if they are allowed to see who has accessed their data, and can question access that they have not authorized. Therefore, we propose a system, presented in Fig. 5, that displays access to EHR data by recipient. Users are able to scroll through multiple categories of health data to see who had accessed which information and when.

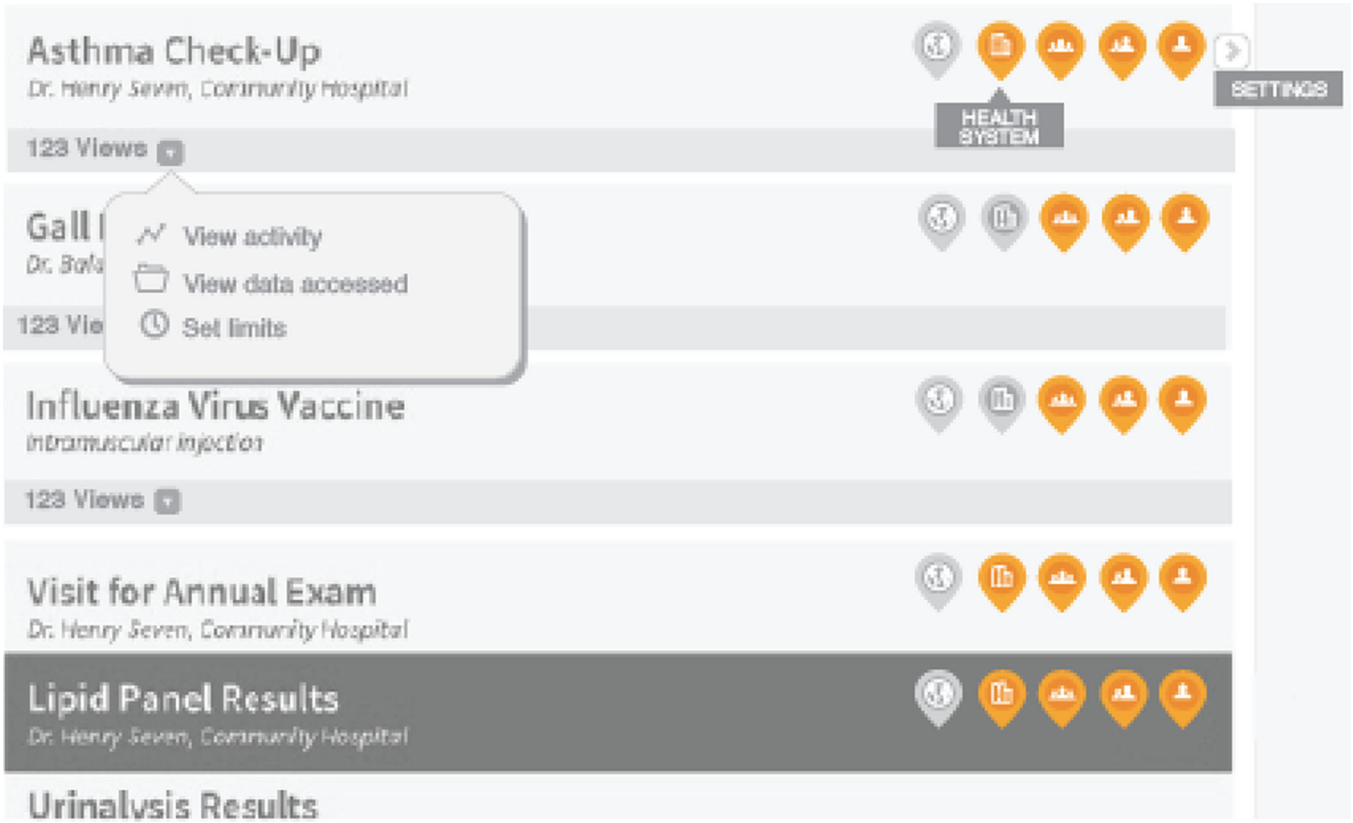

Figure 4. A contextual privacy/sharing control concept adapted from Nightingale, the winner of the ONC and VA's 2012 patient health record design challenge[34]

Summary

Patients overwhelmingly expressed a desire to have access to their own medical records, as well as a desire to control who views their health care data. Without being able to view their data and understand with whom it is shared, controlling access is impossible. Therefore, fulfilling these needs requires both guidelines mandating patient access to and control over their own data, as well as effective and usable design to enable that control.

We have identified UI elements that fulfill the needs we identified. A granular, hierarchical system permits a wide range of customizability while permitting users to allow or restrict access. A time-based access system equips users to restrict information based on collection date. Contextual privacy controls allow users to make sharing decisions in context. Finally, notifying users when their data is accessed and informing them what was accessed has the potential to improve trust in the system, while providing accountability for those who receive patient data.

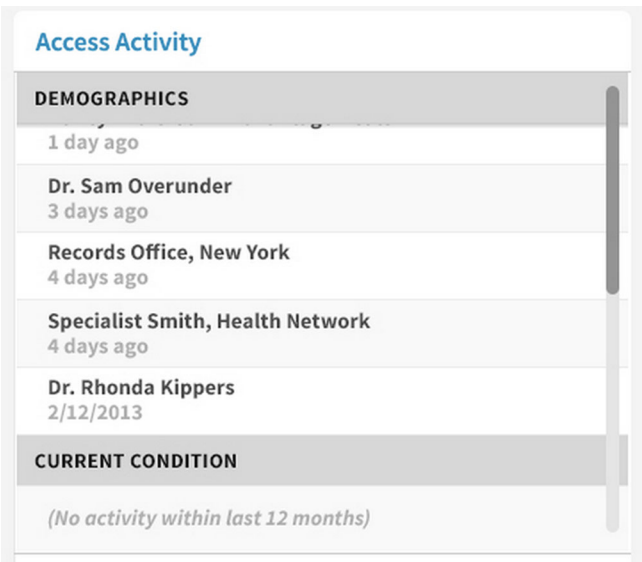

Figure 5. An access notification panel concept that updates with recent accesses organized by category of health information

Limitations

The semi-structured interview method provided the flexibility to explore topics that participants mentioned during the discussion. However, this flexibility necessarily limits the standardization of the interview protocol across participants and generalization of the findings. The benefits of this approach outweigh its associated limitations in that it allowed participants to discuss topics they thought were important, thus providing a patient/data-driven perspective. Future work should seek to refine and corroborate these findings using more structured approaches (e.g., a large-scale survey).

Second, the participant sample is not representative of the US population of patients or patients across the world. Although broad in sociodemographic terms, participants in our sample were all from one hospital system in one geographic area. Furthermore, we oversampled patients with sensitive health conditions because understanding how patients feel about sharing sensitive health information was a goal of our project. Future work should seek to evaluate these findings with a geographically representative sample.

Future Work

Participants discussed many issues that cannot be addressed via a patient-facing interface alone. For example, patients spontaneously expressed the desire for providers to access *only* information that was necessary for their immediate care, a finding echoed in similar research (e.g.,[30]) and implied in[3]; "every consumer, doctor, researcher, and institution has *appropriate access*"). What constitutes "appropriate" access, or better yet, what is optimal for providers to view during any specific care event is an open question. A "data deluge" is not desirable because providers can become overwhelmed by irrelevant details. Previous research has addressed the "minimum data set" necessary to support care,[35] but this concept has not been extended to other populations. Future research should investigate whether the concept of the "minimum data set," which provides the optimal amount and type of information providers need in different medical situations, is feasible across medical conditions. From both a patient and provider perspective, an EHR that provides only necessary information at the right time (i.e., "just-in-time" information) would be ideal.

Similarly, future work must measure the effects of giving patients access control. On the one hand, giving patients control may mean they are more willing to disclose health information. On the other hand, giving patients control may mean that they restrict the sharing of health information in a way that reduces the benefits of EHRs as a coordination/communication tool as well as a tool for health research. A previous study indicated that most patients wanted to be asked for consent before sharing their health information with health researchers.[14] Research is needed to understand how giving patients access and control affects the balance of how much information they provide and share (e.g., EHRs can be double edged swords[6]).

While we have suggested designs that may fulfill patients needs regarding access and control, there is still much research to be done in ensuring thatthese tools are easy to use by patients and serve a useful purpose in the clinical encounter. Towards this end, we intend to explore the effectiveness of privacy "presets" or "templates", i.e., configuration patterns for privacy settings. These can be generated using data from experts in privacy, health care delivery, and government agencies, along with "expert" or trusted patients, and using aggregate decisions from other patients in similar situations or who have a similar privacy profile. These templates would provide scaffolding, making it easier for users to make fast, meaningful privacy decisions about their EHR data (for a related discussion, see[14]).

This paper presents the results of formative user research, intended to generate user needs. The user interfaces presented in this paper resulted from a user-centered approach focusing on usability, ease of use, and usefulness. However, as with all user interfaces, usability can be evaluated and improved—areas in which we continue to work.

CONCLUSIONS

Our study suggests the need for and key characteristics of design of a patient-accessible EHR that places privacy control in the users' hands. We have identified three interaction methods that enable information access control, as well as two specific features that promise to aid the user: contextual privacy controls and access notifications. Patients' preferences were in line with suggestions from ONC HIT and PCAST, a majority of providers (c.f.,[18]) and existing research on patient preferences for the sharing of their electronically stored health information. This suggests that there may be a growing consensus for the need for policies mandating patients' control over their own data, and the need to provide interfaces that allow users to exert control/express their preferences. To meet patient needs, future EHRs must consider these requirements during design. Identifying how patients conceptualize medical records and control access to those records is the first step towards creating an EHR that can preserve and enhance patient privacy by allowing users to express their privacy preferences.

Acknowledgements: *We are grateful to 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, Theda Miller, Chris Power and Marc Overhage. We are also grateful to Laurel Stanley, Dana O'Dell and Andy Van Solkema of VisualHero for their assistance with UI design. We also thank the participants who enthusiastically participated in this study.*

This work was supported in part by grant number 90HT005 from the Office of the National Coordinator for Health Information Technology (ONC), to the Indiana Health Information Technology Corporation, the Center for Law, Ethics and Applied Research in Health Information and the School of Informatics and Computing at Indiana University. EMM is supported by grant #UL1TR001108 from the National Institutes of Health. The opinions expressed in this work are the authors' and do not necessarily reflect the positions of ONC, IHIT, Indiana University, Indiana State University or the Regenstrief Institute, Inc.

Conflict of Interest: *Eric Meslin had a consulting contract within the last 3 years with Eli Lilly & Company on unrelated topics. The remaining authors declare no conflicts of interest.*

Corresponding Author: *Kelly Caine, Ph.D.; Clemson University School of Computing, McAdams Hall, Clemson, SC 29634, USA (e-mail: caine@clemson.edu).*

REFERENCES

1. **Furukawa MF, Patel V, Charles D, Swain M, Mostashari F.** Hospital electronic health information exchange grew substantially in 2008–12. Health Aff (Millwood). 2013;32:1346–54.
2. **Williams C, Mostashari F, Mertz K, Hogin E, Atwal P.** From the Office of the National Coordinator: the strategy for advancing the exchange of health information. Health Aff (Millwood). 2012;31:527–36.
3. President's Council of Advisors on Science and Technology. Report to the President Realizing the Full Potential of Health Information Technology to Improve Healthcare for Americans: The Path Forward [Internet]. White House Office of Science and Technology Policy; 2010 Dec [cited 2014 Sep 15] Available at: http://www.whitehouse.gov/sites/default/files/microsites/ostp/pcast-health-it-report.pdf
4. **Chaudhry B, Wang J, Wu S, et al.** Systematic Review: Impact of Health Information Technology on Quality, Efficiency, and Costs of Medical Care. Ann Intern Med. 2006;144(10):742–52.
5. **Hillestad R, Bigelow J, Bower A, et al.** Can Electronic Medical Record Systems Transform Health Care? Potential Health Benefits, Savings, and Costs. Health Aff. 2005;25(5):1103–17. doi:10.1377/hlthaff.24.5.1103.
6. **Campos-Castillo C, Anthony D.** The double-edged sword of electronic health records: implications for patient disclosure. J Gen Med Inform Assoc. 2014. doi:10.1136/amiajnl-2014-002804.
7. **Bishop L, Holms B.** National Consumer Heath Privacy Survey. Oakland, CA: California HealthCare Foundation; 2005.
8. **Sankar P, Mora S, Merz JF, Jones NL.** Patient Persectives of Medical Confidentiality. J Gen Intern Med. 2003;18(8):656–669.
9. **Meslin EM, Albert S, 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;82:1136–1143.
10. **Meslin E, Schwartz P.** On the sufficiency of using bioethics principles to design patient control of electronic health records. J Gen Intern Med (submitted for publication)
11. **Leventhal JC, Cummins JA, Schwartz PH, Martin DK, Tierney WM.** Patient control of provider access to their electronic health records: Technical and organizational challenges (in press).
12. **Berkwits M, Inui TS.** Making Use of Qualitative Research Techniques. J Gen Intern Med. 1998;13(3):1525–1457. doi:10.1046/j.1525-1497.1998.00054x.
13. **Tong A, Sainsbury P, Craig J.** Consolidated criteria for reporting qualitative research (COREQ): a 32-item checklist for interviews and focus groups. Int J Qual HealthCare. 2007;19(6):349–357. doi:10.1093/intqhc/mzm042.
14. **Caine K, Hanania R.** Patients want granular privacy control over health information in electronic medical records. J Am Med Inform Assoc. 2013;20:7–15. doi:10.1136/amiajnl-2012-00102.
15. **Biondich PG, Grannis SJ.** The Indiana network for patient care: an integrated clinical information system informed by over 30 years of experience. J Public Health Manag Pract 2004; Suppl:S81-6.
16. **Carr J.** Recommendations regarding sensitive health information [Internet]. National Committee on Vital and Health Statistics; 2010 Nov 10 [cited 2014 Mar 28]. Available at: http://www.ncvhs.hhs.gov/101110lt.pdf.
17. INReseearch. Available at: https://www.inresearch.org/home. Accessed 2014 Sep 12.
18. **Tierney WM, Alpert SA, Byrket A, Caine K, Leventhal JC, Meslin EM, Schwartz PH.** Patient Control of Access to their Electronic Health Records: A Real World Demonstration in Primary Care. (in prep)
19. MAXQDA [computer program]. Berlin, Germany: VERBI GmbH; 1995.
20. **Creswell JW, Plano Clark VL, Garrett AL.** Methodological issues in conducting mixed methods research designs. Advances in mixed methods research. 2008:66–83. doi:10.4135/9780857024329
21. Office of the National Coordinator for Health Information Technology. Nationwide privacy and security framework for electronic exchange of individually identifiable health information [Internet]. U.S. Department of Health and Human Services; 2008 Dec 15 [cited 2014 Sep 15]. Available at: http://www.healthit.gov/sites/default/files/nationwide-ps-framework-5.pdf
22. **Berwick DM.** What 'Patient-Centered' Should Mean: Confessions Of An Extremist. Health Aff. 2009;28:4w555–w565. doi:10.1377/hlthaff.28.4.w555.
23. **Safran C, Bloomrosen M, Hammond WE, et al.** Toward a national framework for the secondary use of health data: an American Medical Informatics Association White Paper. J Am Med Inform Assoc. 2007;14(1):1–9.
24. **Delbanco T, Walker J, Bell SK, et al.** Inviting Patients to Read Their Doctor's Notes: A Quasi-experimental Study and a Look Ahead. Ann Intern Med. 2012;157(7):461–470. doi:10.7326/0003-4819-157-7-201210020-00002.
25. **Woods SS, Schwartz E, Tuepker A, et al.** Patient Experience With Full Electronic Access to Health Records and Clinical Notes Through the My HealtheVet Personal Health Record Pilot: Qualitative Study. J Med Internet Res. 2013;15(3):e65. doi:10.2196/jmir.2356.
26. Accenture. Doctors Survey: How Do US Doctors Perceive Healthcare IT [Internet]. Accenture. 2013 May 8. [cited 2014 Sep 15]. Available at: http://www.accenture.com/us-en/Pages/insight-acn-doctors-survey-how-us-doctors-perceive-healthcare-it.aspx
27. **Vodicka E, Mejilla R, Leveille SG, et al.** Online Access to Doctors' Notes: Patient Concerns About Privacy. J Med Internet Res. 2013;15(9):e208.
28. **Kuperman GJ.** Health-information exchange: why are we doing it, and what are we doing? J Am Med Inform Assoc. 2011;18(5):678–82.
29. Data Privacy Lab. theDataMap. Available at: http://thedatamap.org. Accessed 2014 Sep 12.
30. **Whiddett R, Hunter I, Engelbrecht J, et al.** Patients' attitudes towards sharing their health information. Int J Med Inform. 2006;75:530–41.
31. **Teixeira PA, Gordon P, Camhi E, Bakken S.** HIV patients' willingness to share personal health information electronically. Patient Educ Couns. 2011;84:e9–e12.
32. **Damschroder LJ, Pritts JL, Neblo MA, Kalarickal RJ, Creswell JW, Hayward RA.** Patients, privacy and trust: Patients' willingness to allow researchers to access their medical records. Soc Sci Med. 2007;64(1):223–35.
33. **Spiekermann S, Grossklags J, Berendt B.** E-privacy in 2nd Generation E-Commerce: Privacy Preferences versus actual Behavior. Proceedings of the 3rd ACM conference on Electronic Commerce. 2001 Oct 14–17.
34. Office of the National Coordinator of Health Information Technology and the Department of Veterans Affairs [Internet]. Health Design Challenge; c2012 [cited 2014 Sep 15]. Available from: http://healthdesignchallenge.com/
35. **Tierney WM, Beck EJ, Gardner RM, et al.** Viewpoint: a pragmatic approach to constructing a minimum data set for care of patients with HIV in developing countries. J Am Med Inform Assoc. 2006;13(3):253–60.