Designing a System for Patients Controlling Providers' Access to their Electronic Health Records: Organizational and Technical Challenges

Jeremy C. Leventhal, MS[1], Jonathan A. Cummins, MS[1], Peter H. Schwartz, MD, PhD[2,3], Douglas K. Martin, MD[1,2], and William M. Tierney, MD[1,2,3]

[1]Regenstrief Institute, Inc., Indianapolis, IN, USA; [2]Indiana University School of Medicine, Indianapolis, IN, USA; [3]Eskenazi Health, Indianapolis, IN, USA.

BACKGROUND: Electronic health records (EHRs) are proliferating, and financial incentives encourage their use. Applying Fair Information Practice principles to EHRs necessitates balancing patients' rights to control their personal information with providers' data needs to deliver safe, high-quality care. We describe the technical and organizational challenges faced in capturing patients' preferences for patient-controlled EHR access and applying those preferences to an existing EHR.

METHODS: We established an online system for capturing patients' preferences for *who* could view their EHRs (listing all participating clinic providers individually and categorically—physicians, nurses, other staff) and *what* data to redact (none, all, or by specific categories of sensitive data or patient age). We then modified existing data-viewing software serving a state-wide health information exchange and a large urban health system and its primary care clinics to allow patients' preferences to guide data displays to providers.

RESULTS: Patients could allow or restrict data displays to all clinicians and staff in a demonstration primary care clinic, categories of providers (physicians, nurses, others), or individual providers. They could also restrict access to all EHR data or any or all of five categories of sensitive data (mental and reproductive health, sexually transmitted diseases, HIV/AIDS, and substance abuse) and for specific patient ages. The EHR viewer displayed data via reports, data flowsheets, and coded and free text data displayed by Google-like searches. Unless patients recorded restrictions, by default all requested data were displayed to all providers. Data patients wanted restricted were not displayed, with no indication they were redacted. Technical barriers prevented redacting restricted information in free textnotes. The program allowed providers to hit a "Break the Glass" button to override patients' restrictions, recording the date, time, and next screen viewed. Establishing patient-control over EHR data displays was complex and required ethical, clinical, database, and programming expertise and difficult choices to overcome technical and health system constraints.

CONCLUSIONS: Assessing patients' preferences for access to their EHRs and applying them in clinical practice requires wide-ranging technical, clinical, and bioethical

expertise, to make tough choices to overcome significant technical and organization challenges.

INTRODUCTION

The Federal Trade Commission has called for those storing consumer information online to comply with four widely accepted Fair Information Practice Principles: *notifying consumers* about the information being collected and how it is being collected and used; *offering consumers choice* about how their personal identifying information will be used; *providing consumers access* to their online information; and *protecting the security* of the information being collected and stored.[1] Fully applying Fair Information Practice Principles to electronic health records (EHRs) would require giving patients the ability to control who has access to specific information within their EHRs, which could have a number of important clinical, ethical, and legal consequences.[2]

We have previously shown that most patients do desire to have such control over their EHR information but have widely divergent opinions about who should have access and what information they should be able to see.[3] We found that 100 % of patients without sensitive EHR information were willing to provide their primary care physicians (PCPs) with full access to their EHRs, as would 90 % of those with sensitive information. However, only 90 % and 55 %, respectively, would provide access to specialty physicians, 80 % and 40 % would provide access to nurses, and 20 % and 15 % would provide access to researchers. Similarly, clinicians, health system leaders, and patient advocates are also likely to have divergent opinions of the benefits, risks, and impact on patient care from patients' having control over access to their EHRs.[2,4] Although scholars have identified clinical, ethical, and legal challenges in providing patients with control of their

EHR data,[2] there is a paucity of literature describing technical approaches to implementing such a policy. Under contract to the National Coordinator for Health Information Technology, we developed and implemented a system for obtaining and following patients' preferences for EHR access. In this paper, we describe the technical approach we took, the challenges we encountered, and how we dealt with them.

METHODS AND SYSTEM DESIGN PRINCIPLES

Setting

The Regenstrief Institute, established in 1969 to study and improve health systems, was charged to design a "proof of concept" program through which patients could record their preferences for who can see specific information in their EHRs and then implement that system in the Indiana Network for Patient Care (INPC), one of the country's oldest, largest, and most comprehensive health information exchanges.[5,6] We modified Regenstrief's existing program, called Careweb®,[7] which is used to view data in the INPC and the EHR, and is maintained by Regenstrief for Eskenazi Health, a large urban public teaching health system. For this study, we targeted a single Eskenazi primary care clinic where all physicians and clinic staff are employed by Eskenazi Medical Group. No residents or other trainees practice in this clinic.

Designing a program for patients' controlling access to their EHRs requires ethical, legal technical, , and clinical expertise. We therefore created three multidisciplinary project teams: (a) the *Bioethics Team* consisted of bioethicists and clinicians who identified points to consider when designing and implementing a system whereby patients could exercise their rights under Fair Information Practices[2]; (b) the *Patient Preference Team* included informaticists and behavioral scientists who assessed patients' desires for controlling EHR access[3] and designed a user-friendly system for recording their preferences for displaying EHR information[8]; and (c) the *Technical Team* was comprised of Regenstrief Institute EHR developers who created CareWeb[7] and designed and implemented modifications whereby patients' preferences would govern display of their EHR data.

This project had two phases: the first was to design a system for capturing patients' preferences for who can see what data in their EHRs, and the second was to revamp Careweb to use those preferences when displaying EHR data. Although the resulting program was created for the INPC, for this demonstration study we targeted it for use in one Eskenazi Health primary care practice to assess its impact prospectively.

Capturing Patients' Preferences for Displaying their EHR Data

There are tens of thousands of clinicians and non-clinicians who have HIPAA-compliant, password-controlled access to

INPC data. Because many patients are cared for by providers in more than one health system, the INPC downloads and links patients' data across these health systems.[9] Therefore, patients' preferences could affect the display of data captured from multiple health systems. For this study, we limited use to the study primary care clinic.

The study clinic follows an open-access model[10] where patients have an assigned primary care provider (PCP) but are cared for by other physicians, nurse-practitioners, physician assistants, nurses, and other staff. Because these providers often refer patients to other Eskenazi Health providers and clinics, we had to decide which providers would be included. Due to the limited nature of this demonstration study, and to minimize disruption to Eskenazi Health broadly, we limited patients' choices of providers to the nine physicians and 23 staff practicing in the study clinic, and all 23 staff as well as eight of the nine physicians agreed to participate.

In our previous study, most patients wanted their PCP to have full access to all information in their EHRs but would more often restrict access to specialty physicians and other staff.[3] Because our pilot study was conducted in a single primary care clinic, all physicians belonged to a single primary care group, and we had to decide how to display the list of clinic providers to the patients. Most clinic patients know the names of their primary care physicians and clinic nurses but not names of other clinic physicians and staff, any of whom might care for them and all of whom have access to their EHRs. We displayed the list of providers by category and, within each category, by name and allowed patients to select the whole category or each person individually. For simplicity, we grouped providers into three categories: physicians, nurses, and other staff. We arbitrarily included nurse practitioners and physicians' assistants with "other staff" because they fulfill various roles and differ from both physicians and nurses. Careweb contains a provider file for the INPC and Eskenazi Health that includes a field for provider type, which Eskenazi maintains for each provider. Other INPC institutions often do not submit provider details to the INPC, making capturing patients' preferences by provider type difficult.

We previously demonstrated that patients hold widely divergent opinions about sharing their EHR data.[3] Therefore, the Bioethics and Patient Preference Teams recommended giving patients a variety of options for controlling their providers' access to their EHRs. Patients could provide full access to all EHR data to all clinician and non-clinician providers. They could grant access to specific providers and/or specific EHR data. Or they could completely restrict access to all EHR data to all or specified providers. Therefore, the Patient Preference Team suggested giving patients two options: provide or restrict access to all data, to all providers or specific providers, by name or type; or provide/restrict display of only selected sensitive data to all or specified providers.

We had to define "sensitive data," knowing that patients differ greatly in what they feel is sensitive.[3] The recent JASON report from ONC stated that EHRs were too broad and variable for patients to document their preferences for sharing or

redacting sensitive data.[11] It suggested establishing categories of sensitive data that could be used to tag individual EHR data items. Following the recommendations by the National Committee on Vital and Health Statistics,[12] we established five categories of sensitive data: sexually transmitted infections, HIV/AIDS, sexual health and pregnancy, mental health information, and drug or alcohol use and abuse.

In our previous research,[3] patients sometimes wanted to restrict data access based on their age or a range of ages. Because all health systems use birth date as an identifier, patient-selected age ranges could easily be translated into dates that could be compared to the date always attached to each stored EHR item. However, restricting information in clinicians' free-text notes is more difficult. Narrative text could describe events at an age a patient might want to restrict. Restricting such information requires natural language processing (NLP) to "read" the note and redact the restricted information. This is challenging because clinical notes often refer to past history without specific patient ages. For example, a patient having had a pregnancy "as a teen," when the specific event might fall within a restricted age range. For this pilot study, if a patient restricted EHR access based on age, we used the date each item was stored to redact data displays. We did not redact free-text notes. Importantly, when recording their preferences, patients were not told that data redaction would be incomplete, as we felt that explanations of discrete data vs. free-text notes and NLP would be difficult for patients to understand.

Knowing that framing and formatting can affect both patients' and physicians' understanding of risks and benefits,[13] all three project teams spent many hours debating details of displaying patients' EHR access options. For example, should we present such options as "sharing data" or "restricting data access?" We decided that the phrasing should be driven by the default condition: where the default is that clinicians have no routine access to patients' EHRs, the patient preference forms should ask them about sharing their data: i.e. the patient provides access to something that is ordinarily restricted. Where the default is that providers routinely have full access to patients' EHRs, the patient preference forms should ask about restricting access to their data. Prior focus groups with Eskenazi patients showed that they expect their health care providers to have full access to their EHRs.[14] Furthermore, the INPC and all of its member institutions have an opt-out policy: they send all data for all patients to the INPC, where enrolled health care providers have full access to them, unless, when providing consent for treatment, patients opt out of sending their data to the INPC. Therefore, when presenting display options to patients, the form listed providers and categories of EHR data to which they could *restrict* access.

Modifying Careweb to Invoke Patients' Preferences for Data Displays

Careweb builds displays of EHR data from individually stored items, e.g., diagnoses, test results, medications, vital signs, and

other observations. From a technical perspective, redacting discrete data was straightforward because Careweb could simply compare the data a provider has requested to an existing table of patients' preferences. For example, if a provider wanted to view information for a patient with HIV/AIDS who wished to restrict access to HIV/AIDS information for all providers, Careweb could filter out and redact all HIV/AIDS-related diagnoses, test results, and medications. To do this, we had to tag each item in a patient's EHR that fell into the "sensitive" categories listed above. This tagging of sensitive data items was accomplished when Chart Search, Careweb's open-source text indexing and search engine utilizing Solr[15] and Lucene,[16] indexed each EHR term in the patient record being viewed. The index and tags were updated each time a patient's record was opened for viewing. For example, for HIV/AIDS, we tagged all relevant diagnoses (including related diagnoses such as Kaposi's sarcoma or pneumocystis pneumonia that almost exclusively occur in HIV-infected patients), HIV-related diagnostic tests (HIV antibodies, viral loads, CD4 counts, etc.), and antiretroviral drugs that are specific to HIV/AIDS. We also tagged all provider notes written in Eskenazi Health's HIV Clinic.

To restrict data displays for selected providers, we utilized the Provider File maintained by both the INPC and Eskenazi Health. This file contains an entry for all providers for each health system and includes an indication of provider type. Maintaining an accurate, up-to-date designation of provider type can be challenging for large health systems,[17] especially academically affiliated systems where patients can have multiple primary care providers. Fortunately, Eskenazi Health has a 40-year relationship with the Regenstrief Institute[18] and routinely captures provider type. To restrict data displays based on provider, the table of patient preferences was searched for each provider accessing Careweb. If the patient had restricted access to any data for that provider, Careweb invoked those preferences by applying the relevant data filters.

Redacting sensitive data in real health care settings is complex and requires knowledge of clinical medicine, health care delivery systems, and EHRs to make difficult and somewhat arbitrary decisions. For this demonstration study, these decisions were often driven by exigencies such as time and resources available. For example, we could easily restrict display of all HIV Clinic notes, but although Careweb's NLP could redact every mention of HIV/AIDS, its related diagnoses, or antiretroviral medications from all notes and reports, it would be time-consuming and beyond the scope of this project. Such NLP programming would also be beyond the capabilities of most commercial EHRs. Therefore, we chose to restrict displays of free-text notes and reports from restricted care *venues* and provider *specialties* rather than the notes' contents.

Medication records also presented challenges. Drugs often have multiple indications, and the prescriber's intention is rarely recorded on electronic prescriptions or pharmacy records. For example, tricyclic antidepressants are sometimes prescribed to treat neuropathic pain, and some antipsychotic

drugs are sometimes taken as anti-emetics. For our demonstration project, when specific medications were _only_ used in sensitive conditions (e.g., HIV/AIDS), we restricted their display when patients' preferences demanded. We did not redact medications for which there were common indications outside of the sensitive categories. If restricting the display of medications with multiple indications was deemed important, electronic prescribing systems could require physicians to record an indication for such medications.

Diagnostic tests had different challenges. Restricting access to sensitive tests was straightforward when the results were positive, such as pregnancy, HIV, or chlamydia tests. However, restricting access to only positive results could inform providers that the result was positive. Therefore, we redacted all results—positive, negative, and equivocal—for sensitive tests when dictated by patients' preferences. As above, we did not redact test results mentioned in free-text notes.

Patient authentication was a serious challenge. Patients can provide different names (maiden or married names, names with or without middle names or initials, etc.) when registering, and typographical errors occur. It can be challenging to match patients' preferences for EHR access with the correct patient records. Although all commercial EHRs have algorithms for identifying and combining duplicate patient records, their effectiveness is variable. This is even more challenging for health information exchanges storing data from multiple health systems. This was less of a problem for this study in one Eskenazi primary care clinic than the INPC, which imports data from more than 100 hospitals and multiple other institutions. The INPC maintains a Global Patient Registry that stores the medical record numbers for all member health systems in which a patient is registered. A highly accurate patient-matching algorithm created by the Regenstrief Institute[9] merges duplicate records within and among health systems for both Eskenazi Health and the INPC. But it is not perfect, so patients' preferences may not be applied to all of their EHR data. Weeding out duplicate patients takes diligence, and some health systems are more fastidious than others, impacting the effectiveness of programs allowing patient control of EHR access.

We also had to decide whether to inform providers when data was being withheld from Careweb displays. Because one might infer the content of redacted data from knowing it was not being displayed, we chose to redact data without notifying the user. Thus, all Careweb displays appeared the same; providers could not tell whether CareWeb was redacting data displays based on patients' EHR access preferences. However, all clinic providers were informed that some of their patients may restrict access to some or all of their EHR data. Providers were free to discuss this with their patients.

There was consensus among the investigators that patients' preferences should sometimes be overridden, e.g., in emergency situations where patients cannot communicate adequately. Following the iconic statement "break glass in case of emergency," we created a button on Careweb's data display labeled, "Break Glass (Pt Preferences)." Clicking on this button displayed all patient data for that viewing session only. This button was displayed for all patients, whether enrolled in the study or not, but only for the 32 clinic providers enrolled in this study. Otherwise, the button itself might bias the provider's data viewing. For each "break glass" episode, Careweb logged the date, time, patient ID, provider ID, and next screen viewed.

Instead of modifying the basic Careweb program used by all Eskenazi and INPC providers, we could have created a shadow EHR for study patients and removed those items the patient wanted restricted. This may have worked for this small pilot study, but would be impractical for wider use. Having a duplicate EHR for patients preferring to restrict data displays would be cumbersome. Moreover, patients could prefer having different restrictions for different providers, and their data access preferences could change over time. Instead, we chose to modify the Careweb EHR viewer to restrict data displays for specified providers. Careweb contains a middle layer of Core Services that is responsible for processing user data requests (e.g., via Flowsheet or Chart Search), reading the patient preference table and filtering the data displayed to the provider. All the logic around providers, data categories, preferences, and "breaking the glass" was maintained in Careweb's Core Services. The EHR itself was not altered.

RESULTS

Capturing Patients' Preferences

This program was approved by the Indiana University Institutional Review Board. The platform for the patient preference program was the open-source OpenMRS.[19,20] As shown in Fig. 1(a), the form was divided vertically into three sections: "Who," listing participating clinic providers by category (Doctors, Nurses, and Other Staff); "What," giving options to restrict no information, all information, or information in the five sensitive categories listed above; and "When," allowing the patient to enter an age range. A fourth-year medical student with considerable clinical knowledge guided the patient through this form, following a formal written script but also answering questions. The medical student did not explain the potential impact of patients' preferences on health care unless patients asked, which was infrequent. In such instances, he/she merely said that restricting the display of data could affect their care.

Patients used a computer mouse to select their preferences for restricting EHR displays. The Patient Preference Program then displayed the preferences selected on a second page, as shown in Figure 1(b). The two tabs at the top of this form each displayed all of the patients' preferences, sorting them by data categories or people (providers). Each preference was followed by a delete button. If the patient clicked it with the mouse, the display restriction was removed. Final selections were stored in Careweb's preference table.

a

OpenMRS

Tell Us Your Privacy Preferences

Who
Whose access would you like to restrict?

Doctors select all
- ☐ Dr. Jim Stevenson   ☐ Dr. Gregory Samuels
- ☐ Dr. Erica Smith   ☐ Dr. Tom Jones
- ☐ Dr. Lauren Robertson   ☐ Dr. Steve Rhodes

Nurses select all
- ☐ Susan Williamson   ☐ Steven Jefferson
- ☐ Jennifer Smith

Other Staff select all
- ☐ Jeffery Stratford

What
Which information would you like to restrict? ⓘ
- ☐ Restrict No Information
- ☐ Restrict All Information
- ☐ Restrict information on sexually transmitted infections
- ☐ Restrict information on HIV or AIDS
- ☐ Restrict information on sexual health and pregnancy
- ☐ Restrict information on drug and alcohol use or abuse
- ☐ Restrict Mental Health Information

When
For what ages would you like to restrict your information? (Leave blank for all ages)
From [   ] To [   ] years old

[Submit]

b

Current Preferences

| Categories | People |

Category restricted

Restrict Mental Health Information delete
- Dr. Tom Jones from ages 17 to 18 (04/17/1962 - 04/17/1963) delete
- Dr. Steve Rhodes for all ages (all dates) delete

Restrict information on sexual health and pregnancy delete
- Dr. Steve Rhodes for all ages (all dates) delete

Restrict information on sexually transmitted infections delete
- Dr. Tom Jones from ages 17 to 18 (04/17/1962 - 04/17/1963) delete
- Dr. Steve Rhodes for all ages (all dates) delete

Restrict information on drug and alcohol use or abuse delete
- Dr. Steve Rhodes for all ages (all dates) delete

Restrict information on HIV or AIDS delete
- Dr. Steve Rhodes for all ages (all dates) delete

Figure 1. (a): Patient preference program (note: all names are fictitious). (b): Display of patient preferences, displayed at end of dialog (note: all names are fictitious).

Figure 2(a): Chart search screen showing data for a patient allowing access to all data (search term = "alprazolam") (note: all names are fictitious). (b): Chart search screen showing data when "Mental Health" data were restricted (search term = "alprazolam") (note: all names are fictitious). (c): Chart search screen showing data when all data were restricted (search term = "alprazolam") (note: all names are fictitious).


As described in detail in the article by Schwartz et al. in this *JGIM* supplement,[21] slightly more than half of the 105 patients enrolled wanted all physicians, nurses, and clinic staff to view all of their data. Five patients wanted no one to view any information in their EHRs. The remainder restricted access by provider and/or categories of sensitive information. Three patients restricted access to information based on age (late teen years to early-mid adulthood). Providers were not informed which patients were enrolled in the study, or of their preferences.

Applying Patients' Preferences to Careweb Data Displays

Figure 2(a) shows the Careweb main screen. Note that the main menu at the top of this page contains a "Break Glass (Pt Preferences)" button that, once hit, will override any patient-entered data-viewing restrictions for that Careweb session. The data shown in Fig. 2(a) were displayed using Careweb's Chart Search program, a Google-like search engine that searches for terms in discrete data and free-text. Patients' preferences would guide data displays whether using Chart Search, Flowsheet (a chronological flowsheet of all or selected data), or Results (a vertical chronological display of all data). This figure shows the Chart Search display for a patient with no data display restrictions. The search term was "alprazolam," an anti-anxiety medication in the "mental health data" category, which was found in three pharmacy records, two full-text discharge summaries, and a visit note.

Figure 2(b) displays data for the same fictitious patient and the same search term, this time where the patient restricted the display of all "mental health data" to all clinic providers. All alprazolam pharmacy records were redacted. However, the display still contains the three free-text notes containing references to alprazolam.

Figure 2(c) displays data for the same patient and the same search term where the patient restricted access to all EHR data. The resulting display is empty, as if the new patient were new to the health system.
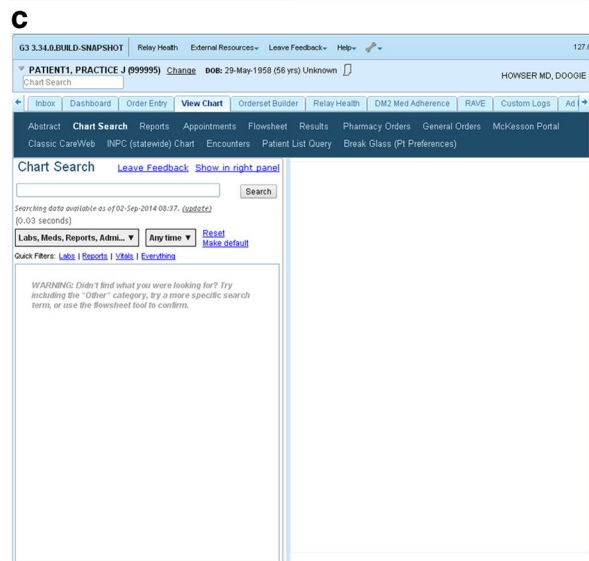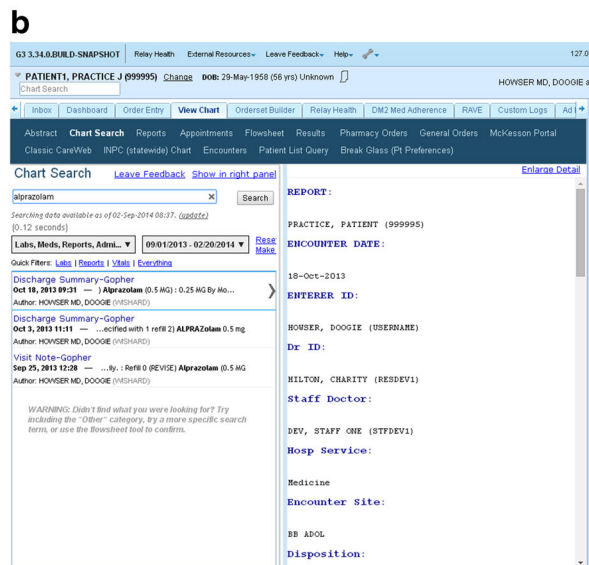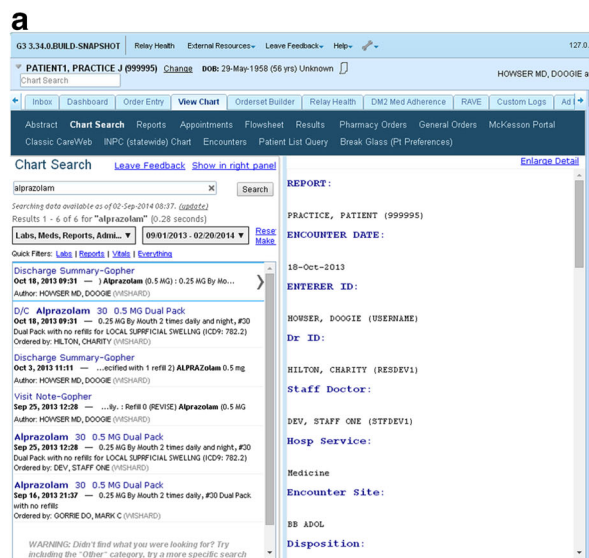
DISCUSSION

Giving patients granular control over who can view their EHR data is complex, requiring clinical, bioethical, informatics, and

programming expertise. Difficult choices are necessary concerning the level of data granularity, how to identify and manage data displays for various types of health care providers, and how to balance clinicians' needs to provide safe, high-quality care with patients' rights under Fair Information Practice Principles. One of this project's investigators (Dr. Schwartz) practiced in the study clinic and helped make sure that the arbitrary decisions we made were consistent with local customs, beliefs, and expectations. Organizational and technical decisions were made easier because this pilot study was conducted in a single clinic. If patient-controlled EHR access were to be implemented for all of Eskenazi Health or the entire INPC, these decisions would require input from health system leaders. They could be applied consistently throughout each health system or could vary for different care venues (inpatient, outpatient), services (e.g., hospital medicine, primary care, specialties, and subspecialties), or providers.

Eskenazi Health and the INPC both use Regenstrief's database platform and data viewer, and the developers were engaged with leaders in both Eskenazi Health and the INPC. (Dr. Tierney was Eskenazi Health's Chief of Internal Medicine and served as Vice Chair of the Board of Directors of the Indiana Health Information Exchange, which manages the INPC.) Without such close partnerships, making decisions for assessing patients' granular EHR control and implementing them would be difficult. This may explain why some health systems are defaulting to "all or none" patient-controlled EHR access, e.g., by patients' entering passwords during visits. The information presented above outlines the difficult decisions and compromises we had to make and that every developer and hosting health system would have to make to implement more thoughtful, granular patient control of EHR access. Such decisions could help strike a balance between meeting patients' preferences for EHR access and providers' needs to provide safe, effective care.

This study had limitations. First, it was performed in a single health system and health information exchange that uses the Regenstrief Institute's unique EHR and data viewing system. Many of Careweb's unique capabilities are not currently available in most commercial EHR systems. However, the Regenstrief Institute has been a pioneer in a number of aspects of EHRs, such as computer-based provider order entry[22] and decision support,[23] that have become required of EHRs to meet meaningful use criteria. By demonstrating Careweb's data management and display capabilities, we hope they will become widely available in commercial EHRs and health information exchanges.

We also found that complete redaction of EHR information as per patients' wishes was impossible. Tagging and redacting discrete items such as diagnoses, tests, and medications was straightforward and should be available in most commercial EHRs. However, redacting information embedded in free-text notes is substantially harder. Although NLP has improved dramatically over the past several years,[24] it is still in its infancy and has not been broadly implemented to extract discrete data locked in free-text notes and reports. Until NLP capabilities are more well-developed and broadly available, complete granular control of access to patients' EHR data will continue to be impossible.

Capturing patients' preferences is not trivial. Health care is complex, with patients visiting multiple providers and systems that may or may not share data. And EHRs are complex, variable, and constantly changing in content and scope. Therefore, simplification is necessary. We relied on the National Committee for Vital and Health Statistics' list of sensitive types of data, but our research suggests that there is no consensus among patients about what is sensitive and should have restricted access.[3,8] Future patient-controlled access systems might query individual patients about aspects of their record that they feel are sensitive and should be restricted. A program, with the help of a clinician, could translate those preferences into a specific set of data items that could be tagged and then updated each time it is opened. (Chart Search updates indexes and tags in less than a second per patient record.) Over time, patients' opinions of what are sensitive data will yield a more comprehensive list.

It will be important to decide what patients should be told when expressing their preferences for EHR access. They should know the completeness of data redaction and have some understanding of the consequences of withholding data from providers. Given that NLP is in its infancy and the risks and benefits of patient granular EHR control are mainly unknown, much urgent research is needed.

Ultimately, overcoming technical and organizational barriers to patient control of EHR access will require a dialog between patient and provider advocates, biomedical informaticians, and regulators such as the National Coordinator for Health Information Technology. Engagement and open dialog are key to balancing patients' desires to control access to their health information with providers' needs for data to deliver high-quality, safe care. Organizational decisions and technical solutions can then follow to balance care management and patient privacy to enhance patient–provider trust and communication.

Corresponding Author: William M. Tierney, MD; Regenstrief Institute, Inc., 401 West Tenth Street, Suite HS2000, Indianapolis, IN 46202, USA (e-mail: wtierney@regenstrief.org).

REFERENCES

1. Federal Trade Commission. Privacy online: Fair information practices in the electronic marketplace: A report to Congress. FTC: 2000; available at: http://www.ftc.gov/sites/default/files/documents/reports/privacy-online-fair-information-practices-electronic-marketplace-federal-trade-commission-report/privacy2000text.pdf; accessed September 23, 2014.

2. **Meslin EM, Alpert SA, Carroll AE, Odell JD, Tierney WM, Schwartz PH.** Giving patients granular control of personal health information: using an ethics 'Points to Consider' to inform informatics system designers. Int J Med Inform. 2013;82:1136–1143.

3. **Caine K, Hanania R.** Patients want granular privacy control over health information in electronic health records. J Am Med Inform Assoc. 2013;20:7–15.

4. President's Council of Advisors on Science & Technology. Report to the President Realizing the Full Potential of Health Information Technology to Improve Healthcare for Americans: A Path Forward. Available at: http://www.whitehouse.gov/sites/default/files/microsites/ostp/pcast-health-it-report.pdf. Accessed September 23, 2014.

5. **McDonald CJ, Overhage JM, Barnes M, et al.** The Indiana network for patient care: a working local health information infrastructure. An example of a working infrastructure collaboration that links data from five health systems and hundreds of millions of entries. Health Aff (Millwood). 2005;24:1214–1220.

6. **Biondich PG, Grannis SJ.** The Indiana network for patient care: an integrated clinical information system informed by over thirty years of experience. J Public Health Manag Pract 2004;Suppl:S81-6.

7. **Duke JD, Morea J, Mamlin B, et al.** Regenstrief Institute's Medical Gopher: A next-generation homegrown electronic medical record system. Int J Med Inform. 2014;83:170–179.

8. **Caine K, Kohn S, Lawrence C, Hanania R, Meslin EM, Tierney WM.** Access, understanding, control, and notification: Implications for the design of a patient-centered tool to allow individual choice in the disclosure of EHR data. J Gen Intern Med 2014 (in press).

9. **Zhu VJ, Overhage MJ, Egg J, Downs SM, Grannis SJ.** An empiric modification to the probabilistic record linkage algorithm using frequency-based weight scaling. J Am Med Inform Assoc. 2009;16(5):738–745.

10. **Subramanian U, Ackermann RT, Brizendine EJ, et al.** Effect of advanced access scheduling on processes and intermediate outcomes of diabetes care and utilization. J Gen Intern Med. 2009;24:327–333.

11. JASON, The MITRE Corporation. A Robust Health Data Infrastructure. Available at: http://healthit.gov/sites/default/files/ptp13-700hhs_white.pdf. Accessed September 23, 2014.

12. Carr JM. National Committee on Vital and Health Statistics Recommendations Regarding Sensitive Health Information. Available at: http://www.ncvhs.hhs.gov/101110lt.pdf. Accessed September 23, 2014.

13. **Perneger TV, Agoritsas T.** Doctors and patients' susceptibility to framing bias: a randomized trial. J Gen Intern Med. 2011;26:1411–1417.

14. **Weinberger M, Murray MD, Marrero DG, et al.** A pharmaceutical care program for patients with reactive airways disease. Am J Health Syst Pharm. 2001;58:791–796.

15. Solr. Available at: http://lucene.apache.org/solr/; accessed September 23, 2014.

16. Lucene. Available at: http://lucene.apache.org/; accessed September 23, 2014.

17. **Vawdrey DK, Wilcox LG, Collins S, et al.** Awareness of the care team in electronic health records. Appl Clin Inform. 2011;2:395–405.

18. **McDonald CJ, Overhage JM, Tierney WM, et al.** The Regenstrief Medical Record System: A quarter century experience. Int J Med Inform. 1999;54:225–253.

19. **Seebregts CJ, Mamlin BW, Biondich PG, et al.** The Open MRS implementers network . Int J Med Inform. 2009;78:711–720.

20. OpenMRS. Available at: http://openmrs.org; accessed September 23, 2014.

21. **Schwartz PH, Caine K, Alpert SA, Meslin EM, Carroll AE, Tierney WM.** Patient preferences to control access to their electronic health records in primary care. J Gen Intern Med 2014 (in press).

22. **Tierney WM, Miller ME, Overhage JM, McDonald CJ.** Physician inpatient order-writing on microcomputer workstations: Effects on resource utilization. JAMA. 1993;269:379–383.

23. **McDonald CJ, Hui SL, Smith DM, et al.** Reminders to physicians from an introspective computer medical record. A two-year randomized trial. Ann Intern Med. 1984;100:130–138.

24. **Friedman C, Rindflesch TC, Corn M.** Natural language processing: state of the art and prospects for significant progress, a workshop sponsored by the National Library of Medicine. J Biomed Inform. 2013;46:765–773.