VISUALIZATION OF PRIVACY FILTERS FOR SHARING PERSONAL HEALTH RECORDS

Edward L. Klein[1] and Jesse M. Heines[2]

[1] University of Massachusetts Lowell, Dept. of Computer Science, Lowell, Massachusetts, U.S.A.

[2] University of Massachusetts Lowell, Dept. of Computer Science, Lowell, Massachusetts, U.S.A.

Abstract
Personal health records (PHRs) may include health data from home-based medical sensor devices and smartphones in personal health monitoring and are therefore well-positioned to be integrated with mobile health applications. They can be shared with patients' medical teams and caregivers through patient portals and social networking applications. Before sharing, however, patients will desire privacy policies that vary based on multiple factors, including the patient's relationship to the audience, the sensitivity of the health data, and the patient's current medical state.

Keywords
Personal Health Records, Sharing Health Data, Privacy Control

Introduction

Personal Health Records (PHRs) enable patients to collect and store electronic health records that originate from a variety of healthcare interactions and medical devices. As depicted in Figure 1, PHRs may be shared through a variety of methods, such as patient portals, social networking applications, and Health Information Exchanges (HIEs). Patients will likely desire privacy policies that can control the sharing of their PHRs. Graphical visualization techniques can improve patients' understanding of how privacy filters govern the sharing of their PHRs.

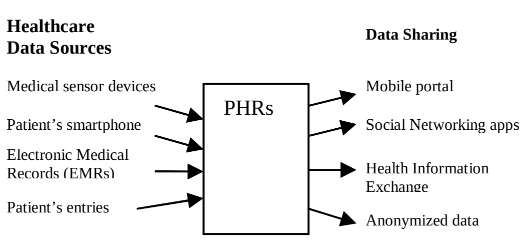

Figure 1: PHR sources and recipients

Some of the sources of healthcare data are shown in Figure 1. Medical sensor devices may be home-based, hospital-based, or entirely mobile through personally attached (wearable) wireless sensor devices. Home-based medical devices are increasingly used to monitor chronically ill patients outside of a hospital setting. Sensing devices can be woven into the physical environment of daily living, through devices attached to a patient's body or embedded in the patient's clothing [3]. Patients can make entries to their PHRs for the level of symptoms as they occur and any other personal observations [5].

Patient consent for the transfer of health data from medical records and devices can be accomplished in a variety of ways [1]. Once the data is in the patient's PHR, sharing is controlled by the patient.

Patients may want to share their health data with a variety of recipients. These recipients can include the patients' doctors, who can receive personal health data through HIEs. Caregivers can receive health data via patient portals, social networking applications, and through smartphone apps. Medical smartphone apps can include software applications used by emergency care personnel. Patients may also share data from their PHRs with sites that collect anonymized health data for analysis of aggregated data, such as the site "Patients Like Me" (www.patientslikeme.com).

Patient sharing of health data will likely be segmented due to the number of different relationships between the patient and the audiences. For example, patients will likely share more information with their closest caregivers. Patients may share health information more widely through healthcare blogs—in particular with their family, friends and other patients that have the same chronic illness.

Patients may also segment sharing based on the sensitivity of their data or their medical status. Some sensitive data may only be shared with select audiences. Patients may share an increased amount of data when they are in a critical or emergency care situation.

The segmented and granular sharing of PHRs requires a number of features in a PHR system. These include: 1) methods for configuring patients' privacy preferences, 2) methods for the enforcement of the privacy controls, 3) and methods for the patient to understand how the privacy controls impact the sharing of their health data. Visualization techniques can improve the patient's understanding of how privacy controls govern the sharing of their PHRs.

Visualization techniques

Several visualization techniques were included in our experiments to try to understand which methods could help patients understand how their privacy settings influence the release of their personal health data.

Future-based health data was simulated in the experiment to help patients understand what data could be generated by medical sensor devices. The health data displayed was specific to the patient's primary diagnosis and treatment phase. The health data is future-based due to the dynamic nature of sensor and mobile devices. This fictional data also included events that occurred in the past, such as doctors' findings and lab results.

Audience-view [6] is a visualization technique used in the experiment which allows users to see what their audience would see. Audience-view is also described as an "emulated" view, since the patient is able to view their PHRs as if they are a member of the viewing audience.

The audience-view visualization technique is supported by color and object transparency to indicate what an audience will and will not see.

A grid system was implemented to enable viewing privacy controls directed at multiple audiences simultaneously [4].

Privacy levels were encoded using commonly understood graphical symbols. Traffic light green-yellow-red symbols indicated data that was: shared, partially shared and data that was not shared. Embedded in each traffic light symbol was an additional graphical symbol indicating the level of sharing: a caution symbol within the yellow traffic symbol to indicate only non-sensitive data shared, and a lock or unlock symbol to indicate data was shared or not shared. Within the health data records the caution symbol was used to indicate sensitive data.

Research Method

This research included a user study which was conducted through a series of fictional tasks executed on an experimental platform. The experimental platfrom was designed to emulate a subset of the features of a Personal Health Record system. The user study was completed in June 2013 with test subjects from an adult living community. Test subjects were asked to complete a fictional task based on a home-based medical monitoring scenario, with fictional data based on patient profiles of a local Visiting Nurse Association (VNA).

User study recruitment

Test subjects were recruited from a local adult living community in Lowell, Massachusetts. This community is made up of active adults age 55 or older, who may be retired or working. In this user study, 73% of the test subjects had no prior experience with PHRs.

Written consent was obtained from each participant, including their consent to be videotaped. The video recordings were used to corroborate interview data and to review test protocols. Each participant received a small ($10 U.S.) gift certificate to a café in appreciation for their time.

Testing environment

The user testing was performed over two days in the clubhouse of the adult living facility. The experimental platform consisted of a commercial laptop computer with mouse and display, running Ubuntu Linux. The platform is based on the Indivo Personally Controlled Health System [2]. Custom features were developed to simulate the generation of PHRs from sensor devices, laboratory results and doctor's findings. Graphical controls were implemented for the test subjects to manipulate privacy controls and observe their impact on the simulated PHRs.

Testing procedure

Demographic data, shown in tables 2-6, was collected prior to the experiments.

Each test subject was read a scripted set of test instructions in order to eliminate variation in the test protocol. Each test subject executed an identical fictional task. The fictional task was based on a patient scenario of the local VNA. In this scenario the patient is undergoing home-based care for recovery following a heart attack. The patient is monitored by a number of medical devices. Data from these devices is uploaded to the VNA's Electronic Medical Record System via the patient's smartphone. These records are then transferred to the patient's PHR system.

In this fictional scenario the patient shares health data with three recipients:

1) Members of the patient's family, who live at a location remote from the patient
2) Friends of the patient, who live locally and assist the patient, as caregivers
3) Viewers of the patient's healthcare blog, which chronicles the patient's healthcare experience

Test subjects were asked to configure privacy controls for each category of simulated health data, and for each recipient. Privacy controls included the level of data sharing, either all data shared, non-sensitive data shared, or no data shared.

Results

Test subects were asked to observe the data shared for each audience based on the configured privacy controls. Data sharing was portrayed in the experimental system as green colored records for shared health data, and transparent white records for health data that was not shared.

Each test subject was asked a set of questions designed to ascertain their subjective reaction to the system. Twenty-two of the thirty test subjects were included in the results due to changes in the test protocol after the first eight subjects, when problems were discovered with the instructions. A majority reported that the visualization techniques helped them visualize what health records will be shared with their social networks. Results varied for individual visualization techniques. Table 1 shows the subjective feedback of test subjects while Tables 2-6 present their demographics.

Table 1: Subjective responses by test subjects

		System Facets			
		Overall	Privacy Filters	Fictional PHRs	Audience View
Subject Responses	Didn't help	2 (9%)	0 (0%)	8 (36%)	1 (5%)
	Helped a little	7 (32%)	5 (23%)	3 (14%)	8 (36%)
	Helped a lot	12 (55%)	15 (68%)	11 (50%)	9 (41%)
	Other (mixed)	1 (5%)	2 (9%)	0 (0%)	4 (18%)

Table 2. Computer skills (self-described).

Basic	Intermediate	Skilled
36%	36%	27%

Table 3. Healthcare interaction experience.

Spouse	Child	Parent
55%	45%	55%

Table 4. Age distribution.

55 to 67	68 or older
32%	68%

Table 5. Gender distribution.

Female	Male
64%	36%

Table 6. PHR experience.

None	Some
73%	26%

Discussion of results

The results from interviews with test subjects indicate that overall 87% of test subjects felt that the visualization techniques helped them visualize how the privacy filters governed the sharing of the PHRs.

Test subjects were asked questions to solicit their subjective feedback for each of the major visualization techniques. Table 1 shows that the privacy filters were considered the most helpful, 68% of respondents felt the privacy filters helped them a lot, and an additional 23% felt they helped a little. 50% of the test subjects felt the fictional PHRs helped a lot, and 41% felt the audience-view feature helped a lot.

Some test subjects commented that they didn't pay much attention to the fictional PHRs because it wasn't really their health data – if they truly suffered from the chronic illness in the fictional scenario, they would have paid more attention to it.

The audience-view was not considered as helpful as the other major features. Some respondents reported that the feature was a great way to depict the information, and they liked the icons used for selecting the audience. Others made comments such as they expected more granular categories – categories were family, friends and others. And some users didn't think the icons were clear enough. Further investigation of these concerns might produce an even more positive response to the audience-view feature.

Conclusion

Data from the user study indicates that graphical visualization techniques can help patients understand how privacy filters control the segmented sharing of their PHRs. The visualization techniques may be implemented individually or in combination. Mobile healthcare applications will likely support configuration of privacy filters directly on mobile devices, and indirectly on other devices, such as personal computers, tablets, etc. Further research is recommended for visualization techniques to be used directly in mobile healthcare applications, which have the additional constraints of mobile devices.

References

[1] Goldstein, Melissa M. *Consumer Consent Options For Electronic Health Information Exchange: Policy Considerations and Analysis*. The George Washington University Medical Center. Accessed September 20, 2013 at: www.healthit.gov/sites/default/files/choicemodelfinal032610.pdf

[2] Indivohealth.org, accessed September 20, 2013.

[3] Jasemian, Yousef. *Sensing of Vital Signs and Transmission Using Wireless Networks. Mobile Health Solutions for Biomedical Applications*, IGI Global 2009.

[4] Lipford, Heather R., Watson, Jason, Whitney, Michael, Froiland, Katherine, Reeder, Robert W. *Visual vs. Compact: A Comparison of Privacy Policy Interfaces.* ACM CHI 2010.

[5] Olla, Phillip and Tan, Joseph. *Personal Health Records Systems Go Mobile: Defining Evaluation Components. In Mobile Health Solutions for Biomedical Applications*, IGI Global, 2009.

[6] Watson, Jason, Whitney, Michael, Lipford Heather R. *Configuring Audience-Oriented Privacy Policies.* ACM SafeConfig 2009.

Edward L. Klein
Department of Computer Science
Ph.D. Candidate
University of Massachusetts Lowell
Olsen Hall, c/o Prof. Jesse M. Heines
1 University Avenue Lowell, MA USA 01854

E-mail: edward_klein@student.uml.edu
Phone: +1.978.934.3620