MeD-Lights: A Usable Metaphor for Patient Controlled Access to Electronic Health Records

Emily K. Adams, Mehool Intwala, Apu Kapadia
School of Informatics and Computing
Indiana University Bloomington
Bloomington, IN, USA
{ekadams, mintwala, kapadia}@indiana.edu

ABSTRACT

Electronic health records (EHR) are poised to replace paper-based medical health records—EHRs show the promise of improving medical care by providing immediate access to a patient's records without having to worry about human-introduced delays. At the same time, mobile devices such as smartphones enable users to maintain their own medical information such as *personal health records (PHR)* as well as control the dissemination and sharing of their EHRs with medical personnel. Deciding what records to share with which medical personnel, however, is complicated by the many different types of records and users' varying privacy preferences. Thus, a usable model is needed to allow users to control the sharing of EHRs.

In this paper we describe and evaluate MeD-Lights, a model that leverages the metaphor of traffic light colors (red, yellow, and green) to portray sensitivity levels of records, and how they should be shared with medical personnel. We implemented a MeD-Lights application on the Android platform and performed a user study using smartphones and show that the semantics of sharing we attach to these colors are indeed intuitive to users and users can use them effectively to manage access to their EHRs.

Categories and Subject Descriptors

D.4.6 [**Operating Systems**]: Security and Protection-Access controls; J.3 [**Life and Medical Sciences**]: Medical Information Systems

General Terms

Security, Human Factors

Keywords

electronic health records, privacy, usability

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. To copy otherwise, to republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee.

IHI'10, November 11–12, 2010, Arlington, Virginia, USA.
Copyright 2010 ACM 978-1-4503-0030-8/10/11 ...$10.00.

1. INTRODUCTION

In today's paper-based medical environment a patient's medical history can generate an extensive paper trail. With the advent of *electronic health record (EHR)* systems the paper-based systems are being replaced with electronic processes. EHR system solutions are being developed to simplify workflows, standardize document formats, and defragment the accumulated paper-based health history of patients.[1] Some popular EHR management solutions include online access to patient's medical history [11] and real-time electronic charting of patient-doctor interaction with mobile devices such as hand-held computers [2]. The patient can view his medical data online on the web while also having the ability to change who can see his health information and medical history.[2] [3]

Managing access to EHRs, however, is challenging. With a plethora of records of different types (depending on the doctor who created the record and the part of the body the record references, for example), users must decide who should be able to access those records. Doing so will be a cumbersome process, and thus a method is needed to simplify how users can share EHRs with medical personnel.

Furthermore, users may not make appropriate decisions while setting such access control policies offline, because they do not have situational information (such as an acute or sudden illness) to make more appropriate decisions according to the context of the situation. Users thus need a mechanism to share EHRs on site during a visit to the doctor. Given the short interaction times, users must be able to make quick decisions to seamlessly share their EHRs while maintaining privacy of sensitive records (for example, a patient might not want to share her oncology records with a dentist). Thus a usable mechanism is needed in which users can effectively set access control policies for a wide range of EHRs in a way that is not burdensome to the user, and also be able to control the sharing of EHRs with medical personnel in dynamic and interactive settings. The key to a successful implementation of a patient-based data access control system is to employ a simple, easy to use interface in which the patient will understand how his data will be accessed and shared. The methodology proposed in this paper empowers the patient by enabling the patient to independently manage personal access control over her EHRs.

To this end, we present an access control model called

[1] IBM®WebSphere®Business Integration Collaborations for Healthcare

[2] Google Health: http://www.google.com/health

[3] Microsoft HealthVault: http://www.healthvault.com/

MeD-Lights (Mobile eHealth Document-Lights), which is based on the intuitive traffic-light metaphor. MeD-Lights introduces a recognizable color-coding scheme of *Red*, *Yellow*, and *Green* as it relates to access protection value of an EHR. This color-scheme can be easily translated to the modes of sharing EHR data: *Green* to share all information; *Yellow* to share only some information; and *Red* to share no information. We believe that this approach will transform a potentially complex access control problem into a simple, easy to understand method for sharing records in most settings. Thus, any patient can be a competent steward of his own health records.

We implemented a MeD-Lights smartphone application on the Google Android smartphone and evaluated MeD-Lights through a user study of 15 subjects. We evaluated both the user's *understanding* of the model (do the semantics of sharing based on colors make sense to users?) and the user's ability to *apply* the model (can the users actually employ this model to control how records are shared?). We find that all participants over varied demographics in our sample fully understood the MeD-Lights model, and were able to use the model with about 90% accuracy.

Contributions.

Our work makes the following contributions:

- We propose MeD-Lights, a usable access control model for controlling access to EHRs in interactive settings, thus empowering users to manage their own EHRs.
- As a proof of concept, we implement MeD-Lights as a smartphone application for the popular Google Android platform.
- We evaluate MeD-Lights through a user study with 15 subjects indicating it is easy to understand and use our proposed access control model.

Paper outline.

In Section 2 we survey the existing environment as it relates to managing EHRs in concrete implementations; in Section 3 we describe our assumed architecture to frame the subsequent description of our model in Section 4; Section 5 explores both qualitative and quantitative results of our user study as well as the effectiveness of out methodology; we discuss subjective ideas generated by this study in Section 6; and we conclude in Section 7.

2. RELATED WORK

With the advent of EHRs, patients have the opportunity to manage their medical records more effectively. The concept of Personally Controlled Health Records (PCHR) [12, 13] has been introduced as "a special class of personal health records (PHRs) distinguished by the extent to which users control record access and contents" [15].

Extending upon the PCHR model, we address user-controlled management of EHRs in a similar fashion. In this paper we will not be making a distinction between PHRs, PCHRs, and EHRs and will collectively refer to all managed health records as EHRs. As described below there are many different solutions created that provide the patient this the ability to define EHR access control based on personal preferences.

Online services like Google Health, Microsoft HealthVault, and Indivo [11][4] seek to develop a system of digitizing and centralizing patients' health data while also making the information globally available through web-accessible interfaces. Through these interfaces a patient can store, itemize, and update health records generated from multiple types of health care entities eliminating the fragmented paper-based collections of patient medical documents. Currently the access model of Google Health and Microsoft Health Vault is an all-or-nothing approach to EHR record access: the patient can choose to allow access to his online health records to a particular person, but cannot change access on a per-record basis.

With the increasing popularity of portable devices and smartphones it is a natural transition to store EHR data on personal devices such as smartphones [6] or on similar devices such as smart cards, PDAs, or USB keys [5, 8, 10]. Similar to the consolidation approach of Google Health and Microsoft HealthVault, some propose also using mobile devices to access EHR records housed on a central server [1].

Some focus on the security of medical data store on and access to EHR via authentication such as biometrics and passwords [6, 14]. As research about securing EHR data is well underway, researchers have begun the transition from focusing on security of data to managing access control of EHRs. There is an increasing trend to apply Role Based Access Control (RBAC) or Discretionary Access Control model to EHR-based doctor-patient interaction resulting in fine grain control over who gets to access health record. [3, 4, 9, 16] A key feature of our access control implementation is the ability for a patient to make dynamic decisions based on the current context, specifically during a doctors appointment.

Our project approaches EHR access control management by augmenting and combining the aforementioned medical record management elements. Like Google Health or Microsoft HealthVault, we implement patient controlled access control, but we extend this model by offering access control at a per-record level. Additionally we implement our usable and intuitive color-coding model of *Red*, *Yellow*, and *Green* to enable the patient to share particular elements of a single record. Finally, as described in Section 3, our smartphone implementation does not require the Internet to access health records while in doctor appointments. The MeD-Lights application allows patients to carry their full EHR database with them, providing freedom to share their EHRs at any time with a medical professional.

Finally, inspiration for this model came from earlier work on "Virtual Walls" [7], which demonstrated that three levels of "transparency" (transparent, translucent, and opaque) were found to be an intuitive way for users to control access to sensor information with friends and family. The MeD-Lights model, however, differs significantly based on the application domain, semantics of sharing, and supporting dynamism.

3. ARCHITECTURE

In the current healthcare system, a patient visits a medical provider and new medical documents are created, which are usually housed in a medical provider's filing system. These documents are referenced on subsequent visits and new records are generated and added to the patient's file.

[4] http://indivohealth.org/

The MeD-Lights application mimics the framework of this paper-based system by providing an interim storage of EHRs generated by visits to a healthcare provider.

Since we are addressing only the usability of the access control model, we make the following security assumptions:

- The EHRs are initially stored securely on cloud servers.
- Contractual agreements between cloud service providers and medical providers are made to comply with HIPAA.
- All channels of communication are encrypted, mutually authenticated and protected for integrity (using TLS for example).
- Once downloaded, the EHRs are encrypted and stored securely on the smartphone.

When the user initially installs the MeD-Lights application, the application communicates with the servers and downloads his EHRs on to the smartphone as shown in Figure 1. The flow of data will be as follows:

1. Storage:

   We assume that the EHRs are downloaded from the servers over a secure communication channel. The original copy of the records will always remain on the cloud servers. Once the health records are downloaded, they are encrypted and stored on the smartphone. Gardner et al. have proposed an architecture using threshold cryptography to securely store health records on smartphone [6].

2. Managing Access:

   Once the health records are stored on the smartphone, the user can access his records at any time. He can check his prescription from his smartphone when he visits a pharmacy or share his records with the doctor during a regular appointment. The user can provide information about his past illnesses to the doctor which will help the doctor to better diagnose his conditions. This takes the pressure off the user in having to maintain, organize and carry all his past records during a doctor's visit. For example, EHRs can be transferred to the doctor via a protocol through the cloud service, or locally via Bluetooth, to a device such as a PDA. The doctor can write her notes of the diagnosis and any prescribed medications before sending the information back to the user's device. We will look at sharing records with the doctor in more detail in the following sections

3. Synchronizing Data:

   Once the doctor's examination is completed and the diagnosis report is received from the doctor, the user can synchronize records back to the servers. Thus, the synchronizing process will ensure the records on the server are updated with the latest information.

In our paper, the primary goal is to make MeD-Lights easy for the user to manage and access his records stored on the smartphone during his routine interaction at a doctor's office. While visiting a doctor, patients may not be comfortable sharing all their EHRs with the doctor. In other words, every patient has his own privacy preference and would consider certain types of records to be sensitive and will share it with only certain doctors. The model that we propose allows the user to select records based on his privacy preference and share them with his doctor.

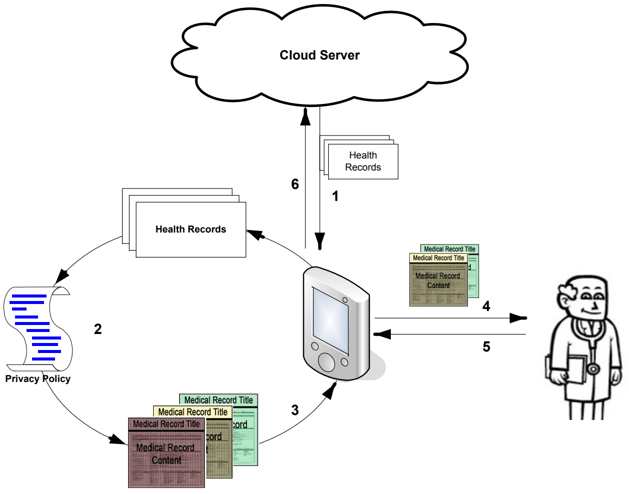


Figure 1: Architecture Diagram – Step 1: The user downloads his EHRs from the cloud server. Step 2: The user's privacy policy is applied to the downloaded EHR data after which each EHR is assigned a color *Red*, *Yellow*, or *Green* color. Step 3: The EHR, now with an assigned color, is stored locally on the smartphone. Step 4: The user transfers his records to the doctor's device during his appointment. Step 5: The doctor may generate a new record and sends it back to the user. Step 6: The user synchronizes the new record with the cloud server.

4. MODEL

In the model, we take an abstract view of the record. Each record is comprised of various *field/value* pairs. We assume three general categories of fields: *Meta-data*, *Title*, and *Content* as outlined in Table 1

The metadata information is used locally for organization and access control. The *Title* contains only brief informa-

Value Type	Example
Metadata:	
Record ID	1, 2, 3, ... 200
Color	*Red*, *Yellow*, or *Green*
Title:	
Title	Broken Arm
Content:	
Record Type	Oncology Records
Body Part	Arm Records
...	...

Table 1: EHR record structure

tion about the record. The *Title* alone does not reveal information about the record itself, but it does contain enough information for the doctor to make a judgment if the record is relevant to the current examination of the patient or not and if she would like to view the record. The *Content* contains the detailed information of the doctor's examination. This would typically contain information such as diagnosis, medical test results and prescriptions from an earlier visit to a doctor. We deliberately leave the other fields for *Content* unspecified as these will depend on how EHRs evolve to a stable schema. For now, we advocate the use of at least the fields listed above to facilitate record-sharing models such as MeD-Lights.

Each record stored on the smartphone has a color associated with it depending on how sensitive the information in the record is. The sensitivity of each record is determined by the user's privacy preferences as discussed in Section 6. The color *Red*, *Yellow*, or *Green* will tell the MeD-Lights application how much information from the record will be shared with the doctor: the entire record i.e. *Title* and the *Content (Green)*, only the *Title* of the record *(Yellow)* or no information *(Red)*.

1. **RED:** Records represented by the color *Red* are records which the user is not comfortable sharing with any doctor. When a record is *Red*, neither the *Title* nor the *Content* information is shared. The user has explicit control over this record and the MeD-Lights application will not share it unless the user specifically take steps in the application to change its color from *Red* to either *Green* or *Yellow*. An example of a *Red* record would be record containing information about breast cancer.

Medical Record Title
Medical Record Content
Not Shared
Not Shared

Figure 2: No information is shared

2. **YELLOW:** Records represented by the color *Yellow* provide only some of the information available in the entire record. When a record is *Yellow*, only the *Title* information is shared (*Content* is not shared). *Yellow* records make the doctor aware that a record exists but the user does not wish to divulge the detailed information.

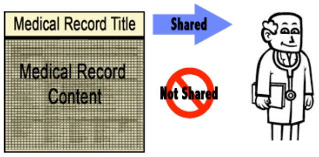


Figure 3: Only *Title* information is shared

3. **GREEN:** Records represented by the color *Green* are records which the user is comfortable sharing with every doctor. When a record is *Green*, the entire record (*Title* and *Content*) is shared with the doctor. An example of a *Green* record is one created when one fractured his arm. One will not be too sensitive about information of the broken arm, and would be comfortable sharing it with all doctors.

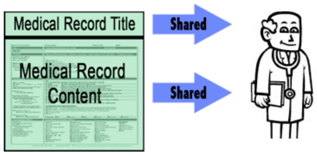


Figure 4: *Title* and *Content* information is shared

We chose the three colored model as it gives us the flexibility and control in selecting records. Also, we show in Section 5 that the model is intuitive and easy to understand for the user. We selected the colors *Red*, *Yellow*, and *Green* as it resembles the colors in the traffic lights. The user can make one-to-one correlation with the colors in the traffic lights and the EHR sensitivity level associated with the record.

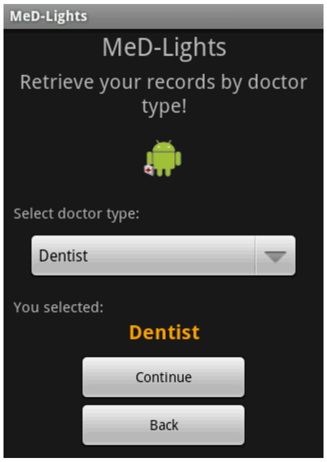
- If the record is colored *Red*, it would indicate to the user to be extremely careful while sharing those records.
- If the record is colored *Yellow*, it would indicate to the user to be cautious while sharing those records.
- If the record is colored *Green*, it would indicate to the user to be at ease while sharing those records.

When the user visits a doctor, he can select records by selecting either the *Doctor Type* or by selecting the *Body Part* in the MeD-Lights interface.

1. **Doctor Type:** The user has the option of selecting records based on *Doctor Type* (Figure 5). By choosing to select records based on *Doctor Type*, all records pertaining to the selected doctor will be retrieved. For example, if the user chooses the doctor type as "Dentist", all records related to the doctor type "Dentist" will be retrieved and presented to the user. The retrieved records will be colored based on the sensitivity preference specified by the user as discussed in Section 6. The user can select the appropriate records which he wishes to share and send it to the doctor.

2. **Body Part:** The user also has the option of retrieving records based on *Body Part* (Figure 6). The user can select the appropriate body part and all records pertaining to the selected body part will be retrieved. For example, if the user chooses the body part "Chest", all records related to the body part "Chest" will be retrieved and presented to the user. The retrieved records will be colored based on the sensitivity preference specified by the user as discussed in Section 6. The user can select the appropriate records which he wishes to share and send it to the doctor.

Once the user has selected records based on either *Doctor Type* or *Body Part*, the user is presented with a summary



MeD-Lights

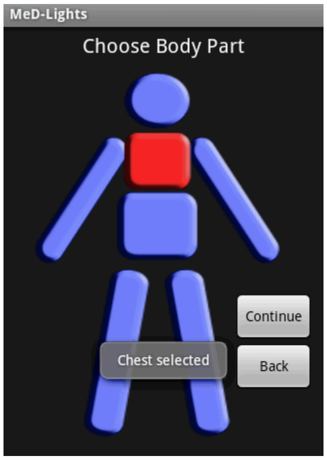
MeD-Lights

Retrieve your records by doctor type!

Select doctor type: Dentist

You selected: Dentist

Figure 5: Selecting records based on *Doctor Type*



MeD-Lights

Choose Body Part

Chest selected

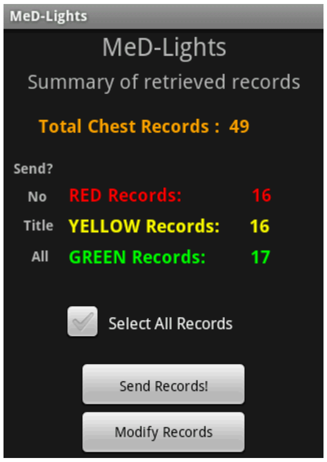
Figure 6: Selecting records based on *Body Part*

page before the records are sent to the doctor (Figure 7). The summary page provides the user with information about what colored records will be shared with the doctor. It also presents the user with three main options as described below:

1. **Default Selection:** Since the records are colored based on the user's sensitivity preference (as discussed in Section 6), the user can choose to share the "Default Selection" to the doctor. The default records are those colored *Yellow* and *Green* from the retrieved record set selected by the user based on either *Doctor Type* or *Body Part*. Records colored *Red* will not be shared at this time.

2. **All Records:** The user has the option of selecting "All Records". "All Records" are records colored *Red*, *Yellow*, and *Green* from the retrieved record set selected by the user based on either *Doctor Type* or *Body Part*.

3. **Modify Records:** The user also has the option of modifying records before sending it to the doctor. The user can choose to modify the color of the record to reflect the amount of information i.e., *Title* and/or *Content* he is willing to share. For example, the user can choose to change the *Red* colored record to *Green* as he would like to send both *Title* and *Content* information to the doctor. The modifications made by the user to the record is only temporary and is only valid for that session.



MeD-Lights

MeD-Lights

Summary of retrieved records

Total Chest Records : 49

Send?		
No	RED Records:	16
Title	YELLOW Records:	16
All	GREEN Records:	17

☑ Select All Records

Figure 7: The summary pages gives the user 3 distinct options to send his records: "Default Selection", "All Records" and "Modify Records"

5. EVALUATION

We first describe our implementation of MeD-Lights for the smartphone, followed by a description of our study design, and the results of our study.

5.1 Implementation

We developed the MeD-Lights application on the Android 1.6 operating system using the Java programming language. The size of the MeD-Lights application on the smartphone is only 264 KB. The patient's simulated EHR database was populated with 200 EHRs (with the schema as described in Section 3) and stored in the native SQLite database on the smartphone. MeD-Lights was tested and deployed on the Android HTC G1 smartphone and study subjects interacted with MeD-Lights on this smartphone.

5.2 Study design

The study comprised of three sections: the first two sections directed the subjects to perform tasks using MeD-Lights on the Android HTC G1 smartphone; the third section was paper-and-pencil based. In each section the subjects were presented with descriptions of simple scenarios as if they were at a doctor's office. The subjects were asked to use the MeD-Lights interface to send records based on "Doctor Type" or "Body Part". Section I of the study tested the subjects' understanding of sharing *all* the retrieved records with the doctor regardless of associated sensitivity level. Section II tested the subjects' understanding of modifying a subset of the retrieved records' sensitivity levels prior to sharing the records with the doctor. The paper-and-pencil based Section III tested the subjects' comprehension of the *Red*, *Yellow*, and *Green* access control model.

- *Section I: Use of the basic interface*

  The goal of this section was to orient the subjects to the MeD-Lights interface and test if subjects were able to simply share *all* their records. Each subject was given a series of scenarios where they were directed to share a set of records retrieved by selecting either *Body Part* or *Doctor Type* regardless of the *Red*, *Yellow*, or *Green* record color. For example, the subjects were asked to imagine they were at the doctor's office and the doctor asked for their "Chest" records. They used the *Body Part* selection page on the MeD-Lights application to retrieve the appropriate "Chest" records and then send all *Red*, *Yellow*, and *Green* "Chest" records regardless of color.

- *Section II: Use of colors*

  The goal of this section was to test the subjects' understanding of how to modify access to records by changing the records' color designations. Each subject was asked to follow the same steps of selecting records as in Section I, however instead of sharing all records the subjects were tasked with modifying some of the retrieved records' colors. For example, the subjects were asked to imagine they were are at the doctor's office and the doctor asked for their "Optometry" records. The subjects were told they were comfortable sharing only some of the "Optometry" records with the doctor. Therefore they used the "Modify Records" page to change their first two *Red* Optometry records to *Yellow*, for example. The subject would confirm the changes and proceed to share the modified set of records.

- *Section III: Understanding the meaning of colors*

  The goal of this paper-based section was to test whether subjects understood the semantics of our *Red*, *Yellow*, or *Green* access control model. This section tested the subjects' understanding of the core concept of what type of information (*Title* or *Content*) would be shared from a record given the record's sensitivity level (*Red*, *Yellow*, or *Green*). For example, the subjects were asked to imagine they were at the optometrist's office. They were told that they had selected the body part as "Head". The subjects were then asked what information from their retrieved *Yellow* Head records will be shared (*Title* or *Content*).

5.3 Subject demographics

We recruited subjects using flyers posted around campus, advertisements on class and departmental e-mail lists. Participation was not restricted to students, and was open to all adults in the community. In total we had 15 subjects. The subjects' age categories ranged from 20–24 to 40–44 (Figure 8) and the distribution of education ranged from "Vocational" to "Doctoral" (Figure 9). Three of the fifteen subjects did not own a smartphone. The average self-rated technical capability was scored as 2 on a scale of one to six with a score of 1 being "Very technical" and a score of 6 being "Not technical at all" (Figure 10).

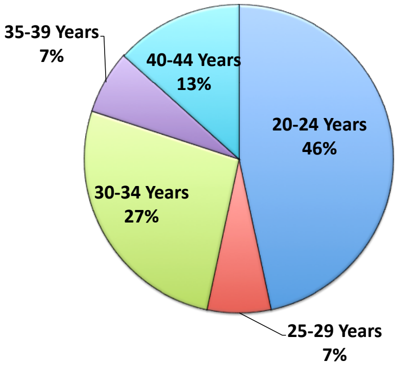


Figure 8: Subjects' age distribution

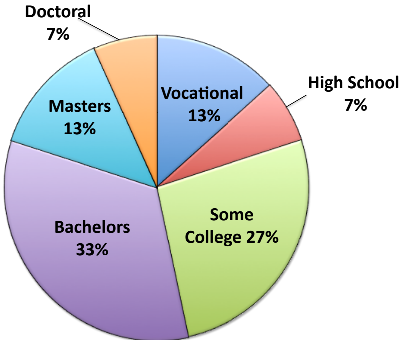


Figure 9: Subjects' education distribution

5.4 Results

As illustrated by Table 2, Section I and Section II scored on average 89% correct (n=13)[5], whereas every subject scored 100% in Section III (n=15) regardless of age, education, perceived technical capabilities, and smartphone ownership. Every subject was able to relate to and mapped our *Red*, *Yellow*, and *Green* model directly to EHR read access.

We now provide more detailed results of our study by breaking down the subjects into different categories. We will not be considering Section III as all subjects scored 100%.

Age: Figure 11 gives the breakdown of the subjects' scores based on age. The subjects involved in the study were aged between 20–49. All of the subjects below the age of 30, answered more than 88% correctly on both Section I and Section II. Subjects aged above 30, answered 90% correctly on Section I and 85% on Section II. This results show that subjects from different age group were able to understand and apply the model to the MeD-Lights application.

Technical Abilities: Figure 12 gives a breakdown of the subjects' scores based on their technical abilities. All subjects in the average to below average group, answered more than 95% correctly on Section I. With only 76% correct answers, it appears that subjects in the above average group had some difficulty with Section I. Subjects in all the groups answered more than 86% correctly on Section II. With almost similar results for above average and below average

[5] Data was not recorded for two subjects in Section I and Section II, thus we did not include the two subjects in the detailed results. The reference of "all" in the Results section are calculated with n=13.

Section	Correct Responses
Section I: Use of the basic interface	89.2%
Section II: Use of colors	89.0%
Section III: Understanding the meaning of colors	100.0%

Table 2: Successful responses by Section

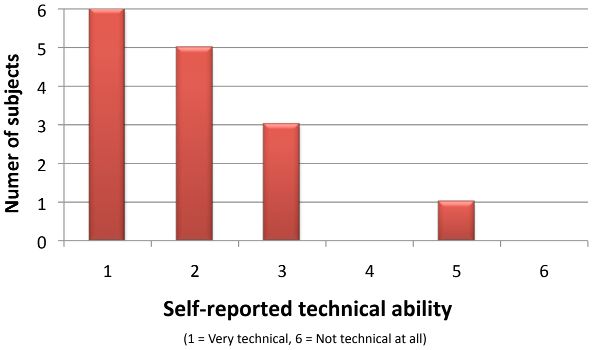


Figure 10: Subjects' self-reported technical ability

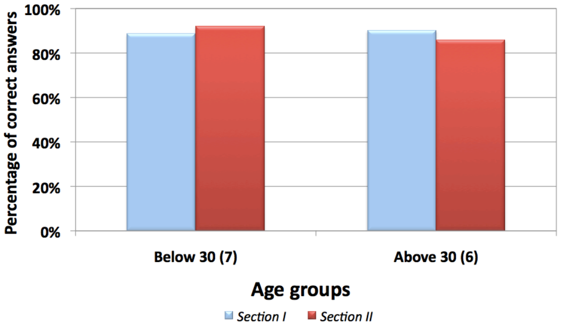


Figure 11: Correct responses for Sections I and II based on age. All age groups answered more than 89% correctly on Section I. Subjects in the age group 40–49 had more difficulty on Section II than other age groups.

groups on Section I and Section II, it goes to show that the model is not complicated and MeD-Lights application does not require specific technical skills.

Education Qualifications: Figure 13 gives a breakdown of the subjects' scores based on their education qualifications. All subjects answered more than 86% of the questions correctly on Section I and more than 88% correctly on Section II. This result once again endorses the usability of the MeD-Lights application and ease of understanding of the model.

5.5 Subjective responses

The study offered subjects the opportunity to provide feedback on MeD-Lights through free-form written comments in the study questionnaire. As reflected in the results of Section III, all the subjects understood the color-coding scheme of *Red*, *Yellow*, and *Green* as it relates to access protection value of an EHR. Three subjects suggested to remove the color text descriptor in the "Modify Record" screen

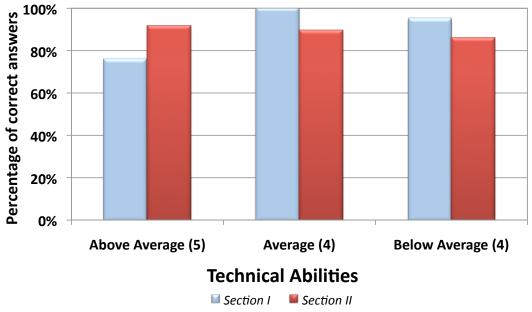


Figure 12: Correct responses for Sections I and II based on technical abilities. Similar results for "Above Average" and "Below Average" groups goes to show that the MeD-Lights is intuitive and does not require specific technical skills.

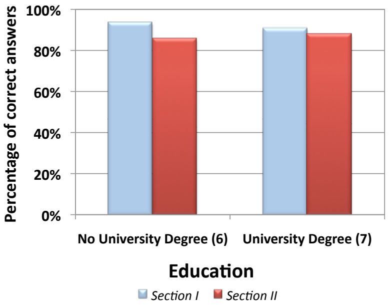


Figure 13: Correct responses for Sections I and II based on education qualifications. Similar results for subjects with "No University Degree" and a "University Degree" shows that the MeD-Lights application was understood by subjects from different education qualifications.

and display colors only. However, considerations must be made for application accessibility thus prominent coloration could still be coupled with the text descriptors. Also the text descriptors will aid in the usability for users with color blindness. Given the subjects' success in Section III and the aforementioned subjects desire to see even more *Red*, *Yellow*, and *Green* color-coding, we can conclude the metaphor for patient controlled access to EHRs is an intuitive and practical model.

Two subjects did not see the need to keep part or all of an EHR from medical personnel. A few of the subjects were concerned with potential sub-standard or incorrect medical care if a patient withheld records from a medical provider. One subject noted that "it's simply dangerous for patients to arbitrarily withhold EHRs from their doctor — most people don't know enough to make good judgments on their medical records." One mentioned that using such a model of patient-controlled health records could be used maliciously to gain the same prescription from different doctors since the EHR associated with such information could be designated as *Red* by the patient. The same subject noted that not sharing potentially sensitive information (for example, a record containing information about a contagious disease) "could be a health risk to their doctor and their staff."

Six subjects had positive comments about the interface: they found MeD-Lights "easy to understand", "fun to learn", and has an "enjoyable interface". One subject appreciated how well the MeD-Lights interface ran and that it "seemed smooth and up to par with app[lication] standards." However, two subjects found it cumbersome to have a large quantity of EHR data on the smartphone and would rather send just a few records instead of the full "Body Type" or "Doctor Type" retrieved record set.

5.6 Limitations of study

Our MeD-Lights study focused on deriving user understanding of the *Red*, *Yellow*, and *Green* model as well as applying the model on a smartphone. The results of our study are based on the responses from 15 subjects. A greater number of study subjects is necessary to generate statistically significant values that can be generalized for the larger population. We did, however, have a good demographic distribution of subjects that was comprised of a diverse group of subjects from different age groups, education qualifications, and technical abilities which avoided heavily biased results.

6. DISCUSSION

Storing EHRs on the smartphone: Due to the sensitive nature of EHRs, and the risks of loss or theft of smartphones, it is essential that EHRs are stored securely on the smartphone protecting the data if the smartphone was lost or stolen. Encrypting and storing the EHR on the smartphone would be secure against the smartphone being lost or stolen. When the patient wants to access his EHRs stored on the smartphone, he would authenticate himself by simply providing his password or biometric information to the smartphone. More complex schemes such as the one outlined by Gardner et al [6] can be used to support multi-authentication schemes including override access by medical personnel in emergency situations.

User suppressing information: Our model provides users with an effective and user friendly way of managing access to EHRs. The user has more control over his EHRs and can select only those records which he is comfortable sharing with the doctor. One may argue, however, that since the user has control over which EHRs he shares with the doctor, the doctor may not be able to correctly diagnose the patient. This is a valid argument, however the same case is possible in the current paper-based patient-doctor interaction. Currently when the patient visits a doctor, the doctor asks a series of questions to the patient. The doctor asks the patient if he has asthma for example. The patient can either accept or deny having asthma. Should the patient choose to hide this information from the doctor, the doctor will not know about the patient's asthma illness unless she examines the patient. We provide the *Yellow* record option to help in such situations where, users are willing to reveal the existence of certain kinds of EHRs. If the doctor thinks such an EHR is relevant to diagnosis she may request the full records from the user and explain why she needs those records.

Simplicity of categories: The MeD-Lights interface uses simple representations of the human body (i.e., no central systems like the nervous system or circulatory systems) and has a limited list of *doctor types*. It remains to be seen if a larger number of categories can be supported while keeping the interface usable, or whether the potentially large number of doctor types would be overwhelming to users.

User setting of privacy preference: One of the ways in which sensitivity levels of EHRs are determined is at storage time when a new, doctor-generated EHR is received by the patient's smartphone. In this case, when the patient receives the diagnosis report and medication information from the doctor, the patient assigns a sensitivity level for the EHR before it is stored on his smartphone. By storing the information at the time of the appointment the patient is in a better position to classify the EHRs sensitivity level. However, the patient may assign sensitivity levels inconsistently or not assign a sensitivity level at all.

To avoid such inconsistencies, privacy preferences could be automatically generated based on a questionnaire-generated filter. The questionnaire would have several questions by which the user specifies his sensitivity preference. This will be a one-time process which the user will have to perform when the MeD-Lights application is first installed. Once the questionnaire is completed sensitivity preference will be applied to each EHR based on the questionnaire filter. Modifications can be made to the questionnaire filter at any time by the user which will reflect across all EHRs thereby maintaining consistency in the EHR database. Such approaches need further research and we leave it to future work.

7. CONCLUSION

We presented and evaluated MeD-Lights, a usable model that allows patients to control access to their EHRs in dynamic settings. EHR-based systems and standards are still in their infancy, and as these systems evolve we argue for more control in the hands of users. While some patients will certainly opt to share all records with medical providers, we believe our system will be beneficial to the segment of users who are concerned about their privacy in this increasingly networked age. It is our hope that further research will explore the interplay between the desire of patients to control access to their records and the need for medical providers to obtain accurate information for diagnosis and treatment.

Acknowledgments

We thank Shaun Deaton, Nathanial Husted, David Kotz, Aarathi Prasad, and our anonymous reviewers for their helpful feedback. We would like to thank Google for providing us with an Android HTC G1 smartphone as part of a larger grant, and the School of Informatics and Computing at Indiana University Bloomington for their financial support. We thank all the subjects who participated in our user study.

8. REFERENCES

[1] A. T. S. Chan, J. Cao, H. Chan, and G. Young. A web-enabled framework for smart card applications in health services. *Commun. ACM*, 44(9):76–82, 2001.

[2] D. F. Criswell and M. L. Parchman. Handheld Computer Use in U.S. Family Practice Residency Programs. *Journal of the American Medical Informatics Association*, 9(1):80–86, 2002.

[3] M. A. C. Dekker and S. Etalle. Audit-based access control for electronic health records. *Electron. Notes Theor. Comput. Sci.*, 168:221–236, 2007.

[4] D. Eyers, J. Bacon, and K. Moody. Oasis role-based access control for electronic health records. *IEE Proceedings - Software*, 153(1):16–23, 2006.

[5] J. Fulcher. The use of smart devices in ehealth. In *ISICT '03: Proceedings of the 1st international symposium on Information and communication technologies*, pages 27–32. Trinity College Dublin, 2003.

[6] R. W. Gardner, S. Garera, M. W. Pagano, M. Green, and A. D. Rubin. Securing medical records on smart phones. In *SPIMACS '09: Proceedings of the first ACM workshop on Security and privacy in medical and home-care systems*, pages 31–40, New York, NY, USA, 2009. ACM.

[7] A. Kapadia, T. Henderson, J. J. Fielding, and D. Kotz. Virtual Walls: Protecting Digital Privacy in Pervasive Environments. In *Proceedings of the Fifth International Conference on Pervasive Computing (Pervasive)*, volume 4480 of *LNCS*, pages 162–179. Springer-Verlag, May 2007.

[8] G. Kardas and E. T. Tunali. Design and implementation of a smart card based healthcare information system. *Computer Methods and Programs in Biomedicine*, 81(1):66 – 78, 2006.

[9] D. L. Lorenzo D. Martino, Qun Ni and E. Bertino. Multi-domain and privacy-aware role based access control in ehealth. In *International Conference on Pervasive Computing Technologies for Healthcare*, 2008.

[10] I. Maglogiannis, N. Apostolopoulos, and P. Tsoukias. Designing and implementing an electronic health record for personal digital assistants. In *Personal Digital Assistants (PDAÕs), International Journal for Quality of Life Research*, pages 63–67, 2004.

[11] K. Mandl, W. Simons, W. Crawford, and J. Abbett. Indivo: a personally controlled health record for health information exchange and communication. *BMC Medical Informatics and Decision Making*, 7(1):25, 2007.

[12] K. D. Mandl, P. Szolovits, I. S. Kohane, D. Markwell, and R. MacDonald. Public standards and patients' control: how to keep electronic medical records accessible but private Commentary: Open approaches to electronic patient records Commentary: A patient's viewpoint. *BMJ*, 322(7281):283–287, 2001.

[13] L. Röstad. An initial model and a discussion of access control in patient controlled health records. *Availability, Reliability and Security, International Conference on*, 0:935–942, 2008.

[14] U. Sax, I. Kohane, and K. D. Mandl. Wireless Technology Infrastructures for Authentication of Patients. *Journal of the American Medical Informatics Association*, 12(3):263–268, 2005.

[15] M. D. Weitzman RE, Kaci L. Acceptability of a personally controlled health record in a community-based setting: Implications for policy and design. *J Med Internet Res.*, 11(1):e14, 2009.

[16] M. Wilikens, S. Feriti, A. Sanna, and M. Masera. A context-related authorization and access control method based on rbac:. In *SACMAT '02: Proceedings of the seventh ACM symposium on Access control models and technologies*, pages 117–124, New York, NY, USA, 2002. ACM.