Exposing privacy concerns in mHealth

Aarathi Prasad, Jacob Sorber, Timothy Stablein, Denise Anthony, David Kotz
Dartmouth College – Institute for Security, Technology and Society

1 Introduction

Mobile health (mHealth) sensing devices can help individuals work towards a healthier lifestyle or allow them to share the collected information with their doctor to diagnose health issues or manage a chronic disease. If these sensors are collecting personal health information while patients are at home or at their workplace, the sensors might record other sensitive information – like the location of their home, when they leave for work, or who they interact with – information that may in some cases be misused. Patients may be concerned about where that information is stored or who has access to it. In this paper, we refer to the users of an mHealth device as *Patients*, whether they use it for disease management or for personal wellness applications, and we refer to the recipient of the shared information as a *consumer*.

We conducted several exploratory focus groups to understand what privacy concerns Patients might have with the collection, storage and sharing of their personal health information, when using mHealth devices. We found that Patients want control over their health information, and we noticed privacy trends that were particular to Patients in the same age group and with similar health experiences.

2 Focus groups

We conducted exploratory focus-group discussions to gain a preliminary understanding about Patients' privacy preferences. We have thus far had eight focus-group sessions with 3-7 participants each, who were college students (aged 19-30), hospital outpatients (aged 80-85), or residents of a retirement community (aged 65-100). Each focus group lasted for not more than 90 minutes and all participants were paid for their time. We chose these groups since we wanted to talk to Patients who have some health experiences – some who have been recently hospitalized and others who are monitored continuously outside the hospital – and Patients who have limited healthcare-related experiences. In the next phase, we will conduct a user study to test individuals' sharing behavior.

Since mHealth devices are not yet common, the focus group participants were presented with hypothetical scenarios where mHealth devices were used. There were four scenarios, in which an mHealth device was used to collect a Patient's personal information (measuring medication intake, diet and exercise, location or social interactions); the collected data was uploaded to a private website and then shared with health providers, family or friends. The scenarios for the young and the old differed in the age of the protagonists and their medical condition, but were similar in every other aspect like the information collected and the manner in which it was collected, stored and shared.

We presented each scenario to the participants, after which they were asked about the advantages and disadvantages of using mHealth sensors in that scenario. They discussed their concerns regarding the collection of the particular health information in each scenario, and whether there were certain times and places when they did not want to collect that information. The participants talked about why they would want to share certain health information types with health providers and family members. They also raised some concerns regarding storage of the collected information.

We recorded the discussions. We coded the discussions manually, and grouped the statements into categories.

3 Results

We summarize comments by type of participant.
Elderly and young participants said that

- They are more comfortable sharing health information with doctors than with family members, since they trust doctors to keep the information confidential.
- Some of them recognized that information might get compromised during transmission and on a private website.
- Third parties, like insurance companies, advertisers and government agents, should not be allowed to access health information without the Patient's (or caregiver's) consent at the time of request.
- Health information can be shared with family mem-

Proceedings of the USENIX Workshop on Health Security (HealthSec).
USENIX Association, August 2011.

bers if the Patient is incapable of making decisions (like young children or elderly patients suffering from chronic illnesses).

- Most of them rated disclosure of diet and exercise information as a greater privacy threat over that of medication tracking, contradicting our expectations, and, all of them were concerned more about the disclosure of location and social interactions than that of medication and diet and exercise. This confirmed our assumption that Patients' privacy concerns may differ depending the information type being monitored.

Elderly participants said that

- They may not always want to share information with family members: a resident of the retirement home felt she wanted to be independent from her family, while one hospital outpatient felt some depressing news contained in the health information might worry his family.
- Doctors might be overwhelmed with irrelevant data (one participant).

Young participants said that

- They would be comfortable sharing their medical information, like information about their medication, with their doctor; privacy concerns arise, however, when devices capture other information about their lives.
- The devices can collect any information, as long as the Patient gives consent and it affects only the Patient. Privacy concerns arise when an individual's information gets recorded by devices carried by others around her, without her consent.
- Patients cannot understand complex privacy laws and they give consent without knowing how it will affect them later.
- Privacy laws keep changing and it is unclear whether the information collected now will still be protected by the laws later.

4 Discussion

The main challenge to building privacy controls for mHealth devices is the wide range of views held by different people. We suggest the following features for a privacy-control interface for an mHealth device:

- *usable*, so that Patients can understand what choices they have and what choices to make,
- *expressive*, so that Patients can express their preferences and decisions,
- *intuitive*, so that Patients can understand it quickly, without any training, and
- *transparent*, so that Patients are aware of what information is being collected, what is being shared, and with whom.

The interface could also provide recommended settings based on the Patient's background. From the focus groups, we discovered that there were some concerns that were specific to Patients who suffered from serious illnesses, distinct from those who were diagnosed with less serious medical conditions. Privacy concerns also vary with age and with the Patients' relationship with their doctor and family members. We expect that it is probable that Patients will have concerns similar to their peers among the focus-group participants. Since every Patient is different, we cannot set preferences for them, but we can provide recommended settings to help Patients make better sharing decisions about their health information.

The interface could provide sensible default settings for the privacy controls, which could be based on the results of the focus groups and with knowledge of the Patient's background and situation. Patients might select the default privacy settings, either because they are not sure of what settings to choose or because they need immediate benefits and have no time to spend on choosing what to share with whom.

The interface should provide access logs, so that the Patient can decide whether more information is being shared than required with a given data consumer, in which case she might want to restrict sharing or she might decide that more information needs to be shared.

The user interface can identify the sensitive content of the information (using annotations or icons), highlight the possible privacy risks that may result from sharing information, show changes occurring to the information, and reveal when the data is accessed and used, and by whom, to help Patients make sharing decisions.

The interface could provide hierarchical privacy controls – controls that allow patients to specify preferences at higher levels easily and drill down to specific details, if they want to.

Building interfaces that can be used easily by all kinds of Patients is a big challenge, especially since every Patient's needs and values are different. There must be a collaboration with privacy and HCI researchers to work towards building a usable privacy controls interface.

Acknowledgements

This paper results from research at the Institute for Security, Technology and Society (ISTS), and is supported by the NSF under Grant Award Number 0910842 and by HHS (SHARP program) under award number 90TR0003-01.