8-2010

Can I Access Your Data? Privacy Management in Mhealth

Aarathi Prasad
Dartmouth College

David Kotz
Dartmouth College, David.F.Kotz@Dartmouth.EDU

Can I access your Data? Privacy Management in mHealth

Aarathi Prasad
Department of Computer Science
Dartmouth College

David Kotz
Institute for Security, Technology, and Society
Dartmouth College

Abstract

Mobile health (mHealth) has become important in the field of healthcare information technology, as patients begin to use mobile medical sensors to record their daily activities and vital signs. Since their medical data is collected by their sensors, the patients may wish to control data collection and distribution, so as to protect their data and share it only when the need arises. It must be possible for patients to grant or deny access to the data on the storage unit (mobile phones or personal health records (PHR)). Thus, an efficient framework is required for managing patient consent electronically, i.e., to allow patients to express their desires about what data to collect, what to store, and how to share. We describe several challenges posed by privacy management in mobile health.

1 Introduction

The Health Insurance Portability and Accountability Act (HIPAA) protects personal health information and provides guidelines for its use and disclosure [1]. The Health Information Technology for Economic and Clinical Health (HITECH) Act improved upon HIPAA to include privacy guidelines for the exchange of electronic protected health information [2]. Medical data is collected when the patient comes to a hospital and this data is maintained as electronic medical records. Most commonly, patients sign a paper consent form that gives the hospital (and its HIPAA-covered partners) complete access to their records.

Doctors can use mobile medical sensors to monitor their patients while they are out of the hospital; individuals may also use such sensors to track their activities and vital signs for personal wellness improvement. Doctors might monitor the patient's health using hospital-owned sensors, during a hospital visit; in this case, a paper consent form would suffice. But, a patient may wish to use his own sensor. The patient may monitor data from time to time and the doctor would need to query the patient, once the data collection starts; or the patient may initiate data collection based on the doctor's request. In these scenarios, the patient should be able to respond to the query and share data, stored on the mobile node or the PHR, with the doctor. Electronic privacy management, however, presents several issues as we describe in this paper.

Presented at HealthSec, August 2010.

Funded in part by NSF Trustworthy Computing award 0910842.

2 Challenges

Consider an example scenario. Helen wears a pedometer [4] to record the distance she travels and the calories burned and this data is periodically sent to her mobile phone for storage. She visits her wellness coach frequently and transfers the data from her mobile phone onto his computer. She wants the coach to analyze her activities and help her work towards a healthy lifestyle. She does not, however, want to share her jogging route, which gets recorded by her mobile phone while it collects pedometer data. In this scenario, Helen wants to be able to decide what types of health information should be shared with her wellness coach.

In another scenario, Jack uploads the data on his sensor to his PHR, which is then shared with his doctor. He is uncertain as to who else will require access to his health information as part of his treatment. Hence Jack delegates to his doctor the right to determine the access policies for all those members of the doctor's staff who might require his medical data. In this case, Jack trusts his doctor. Jack, however, might want to audit his data's access logs to make sure that his doctor did not misuse his trust.

2.1 What data and when to collect

How does the patient determine what data to collect and when [3]? One solution is to collect data at all times and then share only the relevant portions with the doctor, wellness coach or other data consumers. Some patients might feel uncomfortable collecting data continuously; as a privacy measure, they may remove the sensors for some period of time. It is possible, however, that they might forget to put them back on. If we hope patients will wear sensors for extended periods, we need to give them the confidence that they have control over the collection, storage, and sharing of their data.

2.2 Many consumers

Helen and Jack's stories reveal that patients' medical data can be transferred from their sensors to mobile devices or PHRs. The privacy management interface, thus, has to be set up in either the mobile node or the PHR system or both. Helen's wellness coach is the only consumer of her health information. It should be relatively easy, therefore, for Helen to affirm transfer of data from her phone, but there still remains the issue of identifying which data (based on sensor type, time of data collection or other facts) has to be shared. In Jack's case, however, there are many data consumers and Jack has no way of knowing who and what roles will need access to his health records and to what parts of the records. Finally, assigning access rights to all roles will be both time-consuming and error-prone. Jack chose to trust his doctor to grant the proper access privileges to his subordinates, but it is not clear that all patients might be willing to do so.

2.3 Data for doctor vs privacy for patient

We have anecdotal evidence that physicians don't trust patients to make the right decision concerning what data is medically relevant; hence they dont want patients to be given full control over data sharing. They feel that patients should not hide any data since this might lead to a wrong diagnosis and might be fatal. On the other hand, all agree that patients deserve the right to protect their sensitive information. So should patients be allowed to control their health information and, if so, to what degree? The patient can delegate to his doctor the right to make the choice on his behalf. Another solution might be that the doctor's staff could explain the risks and benefits of each option to the patient, to aid in the decision-making process. But can these staff truly understand the patient's privacy needs? They might also be oblivious to non-medical risks and benefits.

2.4 Delete or retain data

What should happen to data once it is no longer required? Should it be deleted (if allowed by the hospital policy) or retained for further reference [3]? If the patient deletes her health records, do all copies get deleted or is a backup retained without her knowledge?

2.5 Query and response formats

A doctor's query might be temporal (request for all health records of the past year), based on a procedure (records related to a recent surgery), or technical (pertaining to the sensor type). Since there can be many such queries, doctors and patients would most likely prefer the query and consent process to be automated. How do you ask a patient for access to his health record? It is difficult to come up with a fixed format for the request, since the nature of queries may vary. While responding to the query, the patient might have to grant or deny access for each of the conditions, which will make the consent process tedious.

2.6 User interface requirements

The interface must allow the patient to revoke or renew the privacy settings later, if required. It should allow (limited) delegation to the doctor, in case the patient is unsure of how and with whom to share his health information. The interface must be usable even by elderly or disabled patients; some patients might be physically challenged or have limited technology background [3]. We can expect many patients to simply select the default options if the interface might be too complicated. The text on the interface must be unambiguous and explained clearly, with limited use of medical terms.

3 Proposed Directions

We list a few features that can be included in the privacy management interface, which could solve some of the above mentioned issues. Introduction of privacy icons [5] in healthcare may help address the usability issue; better comprehension of the privacy risks will increase the patient's confidence, and thus help him make the right choice. The interface documentation can list the different trade-offs and benefits presented by each option. The interface can *recommend* an option that would be beneficial to the patient, based on what the patient's peers have selected. The patient could also delegate to his doctor, as Jack did above, the right to make the choice on his behalf.

4 Summary

The patient has certain legal rights to health-data privacy, to protect his sensitive data and ensure that it is shared only where needed. Patients will not adopt mHealth technologies unless they have confidence in the technology's support for their privacy. On the other hand, patients will not trust, or not use, the technology if the privacy support is too complex to use. Hence it is important that we come up with a usable and efficient interface that tackles the above challenges and makes privacy management effortless.

5 References

[1] HHS. HIPAA website. Online at http://www.hhs.gov/ocr/privacy/ Last accessed April 9, 2010, visited Mar. 2010.

[2] HIPAA Survival Guide. The HITECH Act and HIPAA. Online at http://www.hipaasurvivalguide.com/hipaa-survival-guide-21.php Last accessed April 9, 2010, visited Nov. 2009.

[3] D. Kotz, S. Avancha, and A. Baxi. A privacy framework for mobile health and home-care systems. In *Workshop on Security and Privacy in Medical and Home-Care Systems (SPIMACS)*, pages 1–12, Nov. 2009. DOI 10.1145/1655084.1655086.

[4] Nike Plus. Online at http://www.apple.com/ipod/nike/ Last accessed April 9, 2010, visited 8 April 2010.

[5] A. Raskin. Is a Creative Commons for privacy possible? Online at http://www.azarask.in/blog/post/is-a-creative-commons-for-privacy-possible/ Last accessed April 9, 2010, visited 8 April 2010.