Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 98 (2016) 283 – 289

Procedia Computer Science

The 6th International Conference on Current and Future Trends of Information and Communication Technologies in Healthcare (ICTH 2016)

HIPAA-Compliant Privacy Policy Language for e-Health Applications

Youna Jung[a,]* and Minsoo Kim[a]

[a]*Department of Computer and Information Sciences, Virginia Military Institutue*
425 Mallory Hall, Lexington, Virginia 24450, United States

Abstract

Many e-health applications collect patient's health data and track how they are used by patients to enable and validate their effectiveness. Although e-health applications allow people to access healthcare services in easy and convenient way at the reduced cost, the lack of reliable and effective methods of privacy protection makes people hesitate to use e-health applications, and in turn, it becomes the biggest obstacle to the growth of e-Health applications. To overcome the drawback, in this paper, we first address the lack of consideration of health-related data on existing privacy policy languages and propose the HIPAA profile for existing languages, which contains the Health data schema and extensions to HIPAA-friendly policy languages. By using the HIPAA profile, e-health providers are able to specify HIPAA-compliant privacy policies and patients can express their privacy preferences on not only general usage and user data but also health-related data in detail. For better understanding, we present example policies for e-health applications and patients using the proposed profile.

Peer-review under responsibility of the Program Chairs

Keywords: e-health application; online monitoring; privacy; policy language; HIPAA

1. Introduction

E-health is an emerging area at the intersection of medical informatics, public health, business, and information technologies[1]. By leveraging information technologies, e-health applications provide highly available, user-friendly, and personalized services at reduced cost, regardless of time and place. Currently, many e-health applications are used for diverse purposes, such as online education, healthcare research, healthcare data collection, medical interventions, and health promotion, and they are getting ingrained into the everyday life of people[2,3,4]. To improve the effectiveness of online intervention and/or offer personalized healthcare services, some applications collect detailed, and often identifiable, health data of patients. However, collecting identifiable data on e-health applications become a privacy issue due to the sensitivity of data that e-health applications often deal with. Indiscriminate data collection and/or monitoring may result in serious privacy loss, for examples, patients' private health data may be used for unwanted

* Corresponding author. Tel.: +1-540-464-7498; fax: +1-540-464-7859.
E-mail address: younajung@gmail.com

Peer-review under responsibility of the Program Chairs
doi:10.1016/j.procs.2016.09.044

purposes or shared with unknown people[5,6,7]. In e-health applications, even generic usage data, such as login frequency into an online treatment application, can reveal a patient's medical status.

To protect user privacy in e-health applications, the U.S. federal Health Insurance Portability and Accountability Act (HIPAA)[8] stipulates that the first party of healthcare services must not disclose protected health information to other service entities (HIPAA 164.105.(a)(ii)) with only a few exceptions (HIPAA 164.512). A patient needs to check whether a privacy policy of the e-health application is fully compliant with HIPAA or not, before giving consent to disclose his/her health data. Even if a patient examines an e-health application's policies, the application may behave different from a Service Level Agreement (SLA) that is mutually agreed between a patient and an e-health application. For example, private data can be released regardless of patients' wishes, if a healthcare provider embeds monitoring code and/or third-party data-collecting ads in his/her applications. Although this is an obvious violation of HIPAA rules, there are no solutions that systematically detect the application's fraud and prevent user data from undesirable use and disclosure.

To address the privacy issues on e-health applications, we preliminarily proposed the Privacy-Preserving online Monitoring (PPoM) framework[9] that allows e-health applications to conduct trustworthy user monitoring and enable patients to use e-health applications without concern for loss of privacy. By using the PPoM framework, patients are able to verify user/usage data being monitored through user-friendly interface of web browser and strictly enforce their privacy policies on the client side by controlling outgoing messages sent from users' browsers. However, the performance of the PPoM framework strongly depends on the accuracy and precision of privacy policies. Currently, a patient specifies his/her privacy policies using APPEL[10] or XPref[11], while healthcare service providers use P3P[12]. As general-purpose privacy policy languages, existing policy languages including P3P, APPEL, and XPref focus on generic user/usage data to be used for a variety of online applications and do not give careful consideration to health data. It is therefore impossible for both patients and e-health providers to precisely specify their privacy policies about health-related and/or HIIPAA-related data, and in turn, it lowers the performance of the PPoM framework. To address the lack of consideration of health data in existing privacy policy languages, in this paper, we propose the HIPAA profile which allows an e-health provider to specify a HIPAA-compliant privacy policy and enables a patient to specify his/her privacy preference on health data in detail.

The rest of this paper is organized as follows. In Section 2, we introduce our preliminary work and identify its limitations, and in Section 3, explore existing privacy policy languages and discuss the shortcomings of existing languages. In Section 4, we identify the requirements for privacy policy languages for e-health applications and then propose the HIPAA profile. A use case is presented in Section 5, and we conclude our work in Section 6.

2. Preliminary work

As mentioned above, it is important to monitor patients' health without a violation of privacy in e-health applications. Towards this goal, we proposed the Privacy-Preserving online Monitoring (PPoM) framework that rigorously protects user privacy by referring user policies written in APPEL or XPref and enforcing them on user side during online monitoring[9]. The PPoM framework consists of three components: the PPoM Service, the PPoM Browsers, and the PPoM Tool (PPoMT). The overall architecture is shown in Fig. 1.

- *PPoM Service* – It gathers only authorized data that users allow to monitor. By specifying privacy policies, patients can determine which data can be monitored. User policies will be then enforced by the PPoM Service that selectively collects data based on user policies. Unlike the existing monitoring services where user data are collected based on an application's policies and the policies are enforced by the application itself, the PPoM Service provides a way to enforce user policies during monitoring in a systematic manner rather than simply providing a written agreement.
- *PPoM Browser* – Even if a user is exposed to untrustworthy e-health applications that conduct indiscriminate monitoring in violation of HIPAA and a mutually agreed policy, user privacy must be protected. Towards this end, the PPoM Browser presents all data being monitored and protects user privacy on the user side by blocking outgoing messages which contain data a user does not want to disclose based on a user's policies.
- *PPoM Tool (PPoMT)* – Although patient monitoring is essential, it is difficult for healthcare providers to develop monitoring-enabled applications and privacy policies due to lack of professional IT knowledge. The PPoM Tool (PPoMT) enables non-IT health professionals to specify privacy policies for their healthcare applications through user-friendly interfaces and helps them to convert their existing applications into monitoring-enabled applications.

To use the PPoM framework, first, a provider needs to upload the source code or enter the URL(s) of his/her application to the PPoMT. Then, he/she is required to select objects to be monitored and specify corresponding privacy policies through the interfaces generated by the In-page Selector. The Privacy Policy Generator then creates the application's policies by analyzing selected monitoring data and policies, while the Application Converter updates source code by inserting monitoring code generated by the Monitoring Code Generator into the original source code. The application policies and the updated source code must be deployed in an application server.