Chapter 13
Social Credential-Based Role Recommendation and Patient Privacy Control in Medical Emergency

Soon Ae Chun
CUNY—College of Staten Island, USA

Joon Hee Kwon
Kyonggi University, Korea

Haesung Lee
Kyonggi University, Korea

ABSTRACT

Emerging Health Information Technologies (HIT), such as Electronic Health Records (EHR) and Personal Health Records (PHR) systems, facilitate access to and sharing of patients’ medical data in a distributed environment. The privacy protection of medical information is a pressing issue with the use of these medical technologies. In this paper, the authors present a Patient-controlled Privacy Protection Framework, which allows a patient to specify his or her own privacy policies on their own medical data no matter where they are stored. In addition, the authors extend this basic framework to medical emergency situations, where roles and users may not be limited to an organizational boundary. To enforce patient’s privacy policies even in emergency situations, the authors propose the Situation Role-based Privacy Control model and a social network-based user credential discovery method to recommend a situation role to candidate users. The authors present a mobile prototype system and two experiments to show the feasibility of our approach.

DOI: 10.4018/978-1-4666-2653-9.ch13
INTRODUCTION

Health Information Technology (health IT) holds many promises for the healthcare industry. For example, it promises to provide better care for the patients with lower costs by avoiding unnecessary treatments and promises to allow real time access and sharing of a patient’s records for coordinated care. The major push in health IT is to use EHR (Electronic Health Records) systems that clinical doctors and other healthcare providers can access and retrieve patient records electronically. EHR adoption and diffusion among healthcare providers are currently relatively low, but federal legislations such as the HITECH Act and the HIPAA Act are attempting to accelerate not only the EHR implementation but also the meaningful use of patient data for sharing and for decision support analytics across healthcare providers’ organizational boundaries, urging the use of Health Information Exchange (HIE) standards and an interoperable framework.

One of the many major challenges to overcome for EHR systems to be widely adopted for sharing of patient information across different EHR systems in the HIE environment is ensuring patient privacy. With the use of EHR systems, doctors, other healthcare providers, insurance companies, governments, as well as patients could easily access patient information that is stored in various locations. The patient’s privacy should be a paramount priority. Typically, a patient leaves medical records in various providers’ EHR systems. A general practitioner can enter initial checkup notes and his recommendations on his own EHR system. Then a specialist can also record some patient information in his own EHR system, and so do pharmacists, X-ray technicians, etc. In this distributed environment, it is difficult to ensure the consistent privacy control for different health information of the patient.

Currently, a patient at the initial visit to a doctor’s office fills out a paper-based form regarding the health information privacy on how his or her own health information may be shared. It is difficult to ensure that privacy is controlled in the manner the patient desires or to ensure that the healthcare providers honor the privacy specifications of the patient about sharing and using his or her own health data. The patient simply relies that the organization’s policy is executed in good faith, but has no control over who can access what and how her own data can be shared and used.

In this paper, we first present the patient controlled privacy framework, where a patient can specify and manage her own privacy policies on her own data that are stored in different locations (e.g., doctor’s offices) to maximize the control on the privacy of her own data. In addition, the framework has a privacy policy enforcement component that can control and keep track of the provenance of access, release, sharing and advanced analytics of their medical data such that the patient’s privacy policies are properly adhered to.

However, the basic patient controlled privacy framework may fail in case of a health emergency since the patient’s own policy may not list all the possible emergency situations and non-typical roles may be involved such as the first responders or volunteers who are not in the “regular” healthcare network of the patient. In the absence of pre-specified patient controlled privacy policy in an emergency situation, the system should still be able to provide privacy control, instead of revealing all the medical records unconditionally. To achieve this, we present an approach called Situation-Role based Privacy Control Framework, where a medical emergency situation is modeled with a typical sequence of activities that are associated with handling the medical emergency situation, and a set of default roles for each activity in the situation, called situation roles is defined.

In this framework, the authentication process involves two levels: First, the system should verify the authenticity of the emergency situation. This process is called authentication of situation. Secondly, it should authenticate a person (user) for each activity in the mitigation process such that