Abstract. Recent trends in healthcare delivery have led to a shift towards a patient-centric care model which depends on the evolution of information access and tools beyond Electronic Health Record (EHR) systems controlled by healthcare providers to Personal Health Record (PHR) systems whose architectures are based on the fundamental assumptions that the complete records are centrally stored and that each patient retains authority over access to any portion of his/her record. PHRs offer significant potential to stimulate transformational changes in emergency healthcare delivery since they can provide a complete picture of a person’s healthcare record when and where needed. However, a security issue of prominent importance arises which is concerned with the process of granting (revoking) authorization to (from) healthcare professionals without the patient’s involvement. This paper presents an approach to automating the authorization propagation process in PHR systems by means of context-aware technology, which is used to regulate user access to data via a fine-grained access control mechanism.

Keywords: Personal health records, Information availability, Access control, Emergency, Authorization propagation.

1 Introduction

Throughout their lives individuals receive care in different parts of the health care system. This results in patient health data being scattered around disparate and geographically dispersed information systems hosted by different healthcare providers [1], [2]. The lack of interoperability among these systems impedes optimal care as it leads to unavailability of important information regarding patient health status when this is mostly needed (e.g. in case of an emergency).

Recently there has been a remarkable upsurge in activity surrounding the adoption of Personal Health Record (PHR) systems for patients [2]. A PHR is a consumer-centric approach to making comprehensive electronic medical records (EHRs) available at any point of care while fully protecting patient privacy [3]. Unlike traditional EHRs which are based on the ‘fetch and show’ model, PHRs’ architectures are based on the fundamental assumptions that the complete records are held on a central repository and that each patient retains authority over access to any portion of his/her record [3], [4]. Thus an entire class of interoperability is eliminated since the system
of storing and retrieving essential patient data is no longer fragmented. Hence, quality and safety of patient care is enhanced by providing patients and health professionals with relevant and timely information while ensuring protection and confidentiality of personal data.

Providing patients with access to their electronic health records offers great promise to improve patient health and satisfaction with their care, as well as to improve professional and organizational approaches to health care [4]. Although many benefits have been identified, there are many questions about best practices for the implementation of PHR systems [4]. A number of these questions are related to security issues arising in PHR systems.

As any other EHR system, PHR systems require stringent privacy protections to prevent unauthorized access or use [5][6][7]. Most PHR platforms currently deployed (e.g. Microsoft HealthVault [8], ICW LifeSensor [9]) meet these requirements by assigning the patient with the responsibility of granting access to information comprising his/her health record while access to important information (e.g. blood type, allergies etc) is provided to medical staff in case of an emergency by means of an emergency data set. Although this information is valuable while providing first aid to the patient, a more comprehensive view of the his/her health data is required by the medical staff upon arrival to the emergency department of a hospital.

This paper deals with the particular security issue arising in PHR systems which is concerned with the process of granting (revoking) authorization to (from) healthcare professionals without the patient’s involvement. This security issue is particularly important in managing emergency cases. To deal with this problem, authorization propagation process is automated by means of context-aware technology, which is used to regulate user access to data via a fine-grained access control mechanism. The latter is a role-based, context-aware access control mechanism that incorporates the advantages of broad, role-based permission assignment and administration across object types, as in role-based access control (RBAC) [10], and yet provides the flexibility for automatically adjusting access permissions on a patient’s PHR on the occurrence of unpredictable events (e.g. emergency case).

2 Related Work

During the last few years, there has been a growing interest in the utilization of PHR systems as both patients and healthcare organizations realized that their use may entail a number of benefits, such as better access to information, increased patient satisfaction and continuity of care [2], [4]. However, certain barriers to the integration of PHR systems to the clinical practice have been identified, most of them related to security issues [2], [4]. In recognition of these barriers, a number of mechanisms have been developed in an attempt to address several issues mostly regarding access control over the health data comprising a PHR [6], [7], [11]. Some of them are concerned with the provision of access to important healthcare information in case of an emergency.

In Case of Emergency Personal Health Record (icePHR) [12] and My Personal Health Record (myPHR) [13] are applications which, among others, ensure that life saving information is available when mostly needed (i.e. in case of an emergency).