Abstract

European and American Legislation for protection of medical data agree that the patient has the right to play a pivotal role in the decisions regarding the content and distribution of her/his medical records. The Role Based Access Control (RBAC) model is the most commonly used access control model in healthcare but there are also standards that define guidelines for access control in healthcare.

The aim of this master thesis is to firstly verify if existing standards and RBAC based models comply with legislation requirements regarding patient access as well as customized access to his/her Electronic Health Record (EHR) and secondly to define and propose a patient authorization model based on RBAC to be used and customized by the patient.

A literature review of published material was performed and comprised 22 articles and standards from which 12 were included for analysis. Results of the systematic review show that only two models and two standards include patients as a user of the EHR and only one model and one standard provide the possibility for them to customize access control to their EHR. Existing standards define some guidelines for these issues but they are too generic to be directly applied to real healthcare settings.

The proposed patient authorization model is described within a “Patient’s Healthcare Network” (PHN), and combines several characteristics from ISO 13606-4 standard, RBAC and Administration Role Based Access Control (ARBAC) models, temporal constraints, user delegation and break the glass permissions. The patient will actively manage the roles and permissions as well as give permissions of user delegation to other roles, if necessary.

With this model is expected to start bridging the gap that exists between legislation and what really happens in practice in terms of patients controlling and be actively involved in their healthcare. Future work includes the implementation and evaluation of the proposed model with a specific case study in real healthcare practice.

Keywords: Patient Empowerment, Computer Security, Confidentiality, Electronic Health Records, Role Based Access Control Models and Access Control Standards.