Chapter 7.11
A Trusted System for Sharing Patient Electronic Medical Records in Autonomous Distributed Health Care Systems

Surya Nepal
CSIRO ICT Centre, Australia

John Zic
CSIRO ICT Centre, Australia

Frederic Jaccard
CSIRO ICT Centre, Australia

Gregoire Kraehenbuehl
CSIRO ICT Centre, Australia

ABSTRACT

The problem of assuring secure and confidential access and transfer of medical records in healthcare facilities can be partitioned into (a) secure storage and access of electronic records within a facility and (b) secure transfer of electronic records between facilities. To address the first issue, we propose a new tag-based data model for representation of electronic medical records along with patients' policy statements. This model helps to categorize the patient information as well as express patients' consent for a variety of domains, such as individual practitioner and facility. To address the second issue, this paper proposes a way of establishing a trust relationship between two interacting parties based on emerging trusted computing technologies, and describes its application and implementation in an electronic healthcare system. Our proposed

solutions have been demonstrated by developing a prototype system utilizing trusted computing components.

INTRODUCTION

There is a growing need for sharing patient records among health care providers and their associated facilities, in order to provide the best care and clinical outcomes for patients. Due to the increasing use of information technologies in health care industries, patient records are often produced and shared in an electronic form (Choudhri, Kagal, Joshi, Finin, & Yesha, 2003). The coordination of an individual's health care relies on the sharing of personal health information among health care providers and their facilities, such as clinics, test laboratories, and hospitals. It is well known that there are potential benefits and risks associated with the ease with which patients' electronic medical records may be shared (Task Force on Medical Informatics (TFMI), 1996). The ease of sharing information and its rapid dissemination by information technologies underscores the need to assure that the privacy and security requirements of the patient are met at all times and for all possible situations. For example, patients may not want to share or transfer any of their personal health information, without their knowledge and consent, and may want to retain the rights to both access and transfer of their information.

In order to address the issue of control of private medical information, the CSIRO ICT Centre was involved in the development of an electronic consent (e-consent) model (O'Keefe, Greenfield, & Goodchild, 2005) within the context of the Australian Government Department of Health and Aging (DoHA) Electronic Consent Project (Australian Government Department of Health and Aging (DoHA) Project, 2002). The term e-consent was coined to refer to a mechanism through which patients can express their consent policies for electronic records that are accessed and shared between health care facilities. The e-consent model was developed and demonstrated to stakeholders from the Australian health care sector for work commissioned by the DoHA. The most important outcome of the project is the concept of "placeholders," which were used as a means for ensuring privacy-preserving, anonymous electronic record transfer protocols. We make the following two observations on this e-consent model (referred to as the DoHA e-consent model).

First, any underlying data model must support adequate default consent statements and policies to ensure that the e-consent model can secure the privacy and confidentiality of medical data within a facility. The hierarchical data model used by the DoHA e-consent model has limitations on expressing a default policy set, as well as categorizing electronic patient records. This limitation led to the development of our new tag-based data model. In our model, each electronic medical record has a number of policy tags, which we call *e-tags* (electronic tags). Each e-tag has two fields: *category* and *policy*. The category field categorizes records into different groups, such as heart, head, and AIDS. The policy field, which we call an *e-co* (e-consent), contains a number of policy expressions. Unlike role-based access control (RBAC) (Crook, Ince, & Nuseibeh, 2003; Reid, 2003a) and the DoHA e-consent model, our approach allows the specification of access and transfer permissions in terms of (a) roles, (b) health care facilities, (c) health care providers, and (d) categories of information.

Second, in the DoHA e-consent model, the sender facility has to trust the receiver facility (and vice versa). That is, the sender as well as authenticating the identity of the receiver has to rely on the receiver having the right software and hardware system components and configuration to enforce the sender's policies on privacy and confidentiality. Similarly, the receiver also must ensure that it is always in the correct state and configuration for accepting any incoming