Chapter 8
Identity Management and Audit Trail Support for Privacy Protection in E-Health Networks

Liam Peyton
University of Ottawa, Canada

Jun Hu
University of Ottawa, Canada

ABSTRACT

E-health networks can enable integrated healthcare services and data interoperability in the form of electronic health records accessible via Internet technology. Efficiency and quality of care can be improved for example by: streamlining administrative processes involving prescriptions and insurance payments; providing remote access to specialists through telemedicine; or correlating data from clinics, pharmacies and emergency rooms to detect potential adverse events. However, a major requirement to enable adoption of e-health networks is the ability to address issues around security, privacy and trust in a systematic manner. In particular, privacy legislation, regulatory guidelines, and organizational policies require that a framework for privacy protection must be established. Federated identity management can be used to systematically protect patient and health care provider identities in a single sign on framework that controls access to patient data, but an audit trail and reporting mechanism is needed in order to ensure and validate compliance. In this chapter, the authors use example e-health scenarios to analyze the legal, business and technical issues that need to be addressed.

INTRODUCTION

E-health networks can enable integrated healthcare services and data interoperability in the form of electronic health records accessible via Internet technology. Efficiency and quality of care can be improved for example by: streamlining administrative processes involving prescriptions and insurance payments; providing remote access to specialists through telemedicine; or correlating data from clinics, pharmacies and emergency rooms to detect potential adverse events. However, a major requirement to enable adoption of e-health networks is the ability to address issues around security, privacy and trust in a systematic manner. In particular, privacy legislation, regulatory

DOI: 10.4018/978-1-61692-895-7.ch008

guidelines, and organizational policies require that a framework for privacy protection must be established.

The Liberty Alliance project is a consortium of technology vendors and consumer-facing enterprises which is developing an open standard and set of specifications for federated identity management (Tourzan and Koga, 2006). A "Circle of Trust" (CoT) (Shin et al, 2004) is a key concept in which federated identity management is used to create a business to business (B2B) network of cooperating enterprises that provide integrated services to users. These cooperating enterprises have trust relationships and operational agreements established amongst them. Health care networks involve separate cooperating enterprises (physician, hospital, pharmacy, lab, insurance, etc.). Federated identity management is a mechanism that could be leveraged to systematically protect patient and health care provider identities in a single sign on framework that controls access to patient data.

An example scenario of how a CoT could streamline and improve health care services based on an ePrescription service and the processing of insurance payments is described and analyzed in (Peyton et al, 2007). Another scenario based on a CoT shows how data could be integrated from pharmacies, clinics and emergency rooms to support data mining for the detection of adverse events (Hu et al, 2008). Another significant scenario for e-health networks and federated identity management is a telemedicine consultation in which a remote expert is given permission in order to assist in the care of a patient (Peyton and Hu, 2007; Peyton, Hu and Zhan, 2007). This scenario is significant, since it emphasizes the dynamic nature of health care and the balance that must be struck between protecting sensitive health information and ensuring information is immediately available to health care providers as needed in order to provide the highest possible quality of care.

We will use a telemedicine scenario in which physicians consult and provide health services through an online collaborative medical consultation system to highlight the business, legal and technical issues that must be addressed in order to manage privacy compliance in an e-health network. In particular, we review and evaluate the architecture of a Circle of Trust (CoT) focusing on three components defined by the Liberty Alliance framework (Discovery Service, Identity Mapping Service, Interaction Service) as well as a fourth component (Audit Service) that has been proposed as an extension to address potential privacy breaches in Liberty Alliance (Alsaleh and Adams, 2006).

BACKGROUND

A number of researchers have investigated collaborative on-line medical consultation. CoMed (Sung et al., 2000) is a desktop conferencing application, which allows interactive real-time cooperation among several medical experts. A Web-based medical collaboration environment in the context of the regional healthcare network of Crete is described in (Tsiknakis et al, 2002) that provides integrated services for virtual workspaces, annotations, e-mail, and on-line collaboration. The development of a provincial telemedicine center in China is described in (Xiaomin et al, 2002). A web-based system to provide tele-consultation for severe acute respiratory syndrome (SARS) patients in Shanghai Infection Hospital and Xinhua Hospital is described in (Zhang et al, 2005). A summary of legal issues related to telemedicine is given in (White, 2002).

Europe has comprehensive privacy legislation known as the European Union Directive on Privacy and Electronic Communication (European Union, 2002) and Canada has a similar legislation known as the Personal Information Protection and Electronic Documents Act (PIPEDA, 2000). In Ontario, Canada, there is specific legislation for