Chapter 4
Improving Security Policy Coverage in Healthcare

Rafae Bhatti
Oracle Corp, USA

Tyrone Grandison
IBM Almaden Research Center, USA

ABSTRACT

With the adoption of Electronic Medical Records (EMRs), an increasing number of health-related Web applications are now available to consumers, providers and partners. While this transformation offers huge benefits, there are security and privacy concerns integral to the process of electronic healthcare delivery. In this work, the authors first survey the body of evidence to emphasize the design of appropriate security solutions for electronic healthcare applications. The successful solutions will always comply with the prime directive of healthcare - "nothing should interfere with delivery of care" (Grandison and Davis, 2007). The authors then formally present the problem of reconciling security and privacy policies with the actual healthcare workflow, which we refer to as the policy coverage problem. They outline a technical solution to the problem based on the concept of policy refinement, and develop a privacy protection architecture called PRIMA. They also offer guidelines for electronic healthcare applications to ensure adequate policy coverage. The ultimate goal is that electronic healthcare applications should be made secure without compromising usability.

INTRODUCTION

The use of Clinical Information Systems (CIS) in healthcare is gaining prominence, and several government-led mandates and incentives have driven the push toward the implementation of Electronic Medical Records (EMRs). As a result, the CIS managed by healthcare providers has gradually evolved from an isolated database system to an online information portal; offering a new range of possibility in health-related Web-applications to consumers, providers, and partners. While this transformation offers huge economic and technological benefits to the healthcare industry and community, there are security and privacy concerns integral to the delivery of

DOI: 10.4018/978-1-61692-895-7.ch004

care. The adoption of Web-based CIS applications therefore accentuates these concerns, which must be adequately addressed if these applications are to be adopted by patients and used long term. While security solutions for distributed systems abound, a one-size-fits all approach does not suit CIS. This is because healthcare applications have very low tolerance for impediments in the process of healthcare delivery. In contrast to typical online applications where it is reasonable to fit generic security controls to restrict access, healthcare applications require security controls designed specifically with consideration of the healthcare workflow.

Currently, security and privacy management is one of the main inhibitors of the deployment, adoption and use of EMR in the healthcare industry. There has been a recent push in the direction of increasing security and privacy for the health information of patients. The U.S. Healthcare Information Technology Standards Panel (HITSP) is developing standards for EMR that balance patient's rights to control their information and keep it confidential against the needs of healthcare providers and other stakeholders (Wagner, 2009). Leading privacy rights advocates agree that patients should have complete control of their medical records (Wagner, 2009). Several privacy laws and regulations have also emerged around the world in the past few years (Wong 2006), such as the Personal Data Protection Law (JMIA-CICP, 2003) in Japan, the Health Insurance Portability and Accountability Act (HIPAA) in the United States (HHS, 1996) and the Personal Information Protection and Electronic Documents Act (OPCC, 2010) in Canada. For American healthcare, HIPAA is normally assumed to provide the baseline for privacy compliance for healthcare entities.

While HIPAA and other healthcare-related privacy laws and regulations make it mandatory for organizations to specify and publish privacy policies regarding the use and disclosure of personal health information, recent media and academic reports about healthcare privacy (Pear, 2007) (Rostad and Edsburg, 2006) indicate that there is not necessarily a strong correlation between the use of privacy policies and adequate patient privacy protection for electronic healthcare applications. A key reason for this discrepancy is the current state of CIS. Though today's clinical systems may be adequate in handling decision support, that is only one component of a CIS, and it does not account for patient-provider interactions, which permeate the healthcare domain (Malin et al., 2009). The authors in (Rothschild et al., 2005) emphasize the importance of designing information systems that are better aligned with the clinical workflow to allow integrated and patient-centered healthcare delivery. As noted in the literature (Grandison and Davis, 2007) (Malin et al., 2009), the design of CIS should take into consideration the specific constraints related not only to procedural policies but also to the access policies. While the former are related to timely delivery of healthcare information, the latter mandate particular disclosure rules for patients and healthcare providers. Patrick (2009) observes that any disruptions in clinical workflow caused by the technology designed to enforce either procedural or access policies can actually result in reduced overall efficiency and satisfaction, which is the opposite of the original intent of these technologies.

It is a direct result of the shortcomings in current healthcare systems that enforcing the disclosure rules often comes in the way of delivery of healthcare; with the result being that privacy protection policies are often bypassed and are flagged as exception-based accesses in order to deliver care (Rostad and Edsburg, 2006). The primary conclusion from all these observations in the field is that the models used and the policies in place to ensure security of health information and protect privacy of patients are being rendered effectively useless (Grandison and Davis, 2007). Secondly, there is an over-reliance on a secondary infrastructure comprising of audit logs to record exception-based accesses, as opposed to the system being able to incorporate legitimate accesses into