Chapter 8

Regulatory Compliance and the Correlation to Privacy Protection in Healthcare

Tyrone Grandison
IBM Almaden Research Center, USA

Rafae Bhatti
Oracle Corporation, USA

ABSTRACT

Recent government-led efforts and industry-sponsored privacy initiatives in the healthcare sector have received heightened publicity. The current set of privacy legislation mandates that all parties involved in the delivery of care specify and publish privacy policies regarding the use and disclosure of personal health information. The authors' study of actual healthcare privacy policies indicates that the vague representations in published privacy policies are not strongly correlated with adequate privacy protection for the patient. This phenomenon is not due to a lack of available technology to enforce privacy policies, but rather to the will of the healthcare entities to enforce strong privacy protections and their interpretation of minimum compliance obligations. Using available information systems and data mining techniques, this article describes an infrastructure for privacy protection based on the idea of policy refinement to allow the transition from the current state of perceived to be privacy-preserving systems to actually privacy-preserving systems.

INTRODUCTION

In the healthcare industry, privacy concerns are among the main inhibitors to the deployment and use of electronic records systems. In the last decade, the increase in the number of data breaches (Privacy Rights Clearinghouse, 2009) has led to an increase in the number of companies who are concerned about data and brand protection, which has translated into increased spending on healthcare privacy compliance efforts. In the United States, the Health Insurance Portability and Accountability Act (U.S. Department of Health and Human Services, 1996), the new security and privacy requirements imposed by the Health Information Technology for Economic and Clini-
Regulatory Compliance and the Correlation to Privacy Protection in Healthcare

cal Health Act² (U.S., 2009) and the changes to HIPAA mandated by the American Reinvestment and Recovery Act³ (U.S.A., 2009) are normally assumed to provide the baseline for privacy compliance for healthcare entities.

As healthcare organizations implement the required privacy policies, what remains to be ascertained is the impact these policies have on the improvement of privacy practices. More specifically, we address the question: How well does the use of privacy policies translate into good privacy practices? The use of privacy policies refers to the specification, notification and enforcement of policy; while privacy practices refer to the processes and mechanisms (i.e. technological and otherwise) that enable the safe handling of sensitive information.

The answer to our question lies in the design and enforceability of the policy itself. As we will reveal, a policy may be designed to cover all the relevant provisions of the regulation, and yet may still be vague enough to afford very little privacy protection to the patient. We will discuss this further in a later section. Concerns about the inadequate state of privacy protection despite the enactment of data protection regulations have long existed in mainstream media (Pear, 2009). In addition to design issues, studies also indicate that the enforcement of policies governing the use of protected patient information in current healthcare information systems is also lax and that policy is often bypassed or subverted during regular operation (Rostad & Edsburg, 2006).

This scenario makes it possible to purport compliance with privacy regulations, while engendering a false sense of security (or more aptly, a false sense of privacy) among patients. It makes the existence of a policy, in the first place, insignificant; as it does not precisely represent the company’s true stance on data protection. Also, this undermines the notion of empowering the patient, as his consent to a policy is no longer a genuine reflection of the company’s privacy practices. In an electronic health records environment, this conundrum highlights the need for privacy enhancing technology. No prior work has investigated how stated privacy policies measure up to the levels of protection required to truly ensure the safety of patient data, and whether the current system can be elevated from one that purports regulatory compliance to one that really safeguards the privacy of healthcare data. Our goal is to contribute to the solution of this pressing need.

We believe that it is possible, and desirable, to define appropriate mechanisms to ensure that privacy protection moves from the adherence to minimum standards to a level that truly reflects good privacy protection for patients. In this paper, we first evaluate the current HIPPA-inspired privacy practices against the needs of the patient and then present a privacy management architecture called PRIMA that enables refinement of privacy policies based on actual practices of the organization. Policy refinement helps mitigate the stated conundrum because it allows one to (i) improve the design of the policies in order to elevate the level of privacy protection afforded to the patient, and (ii) better align the policies with actual privacy practices of the organization.

The rest of the paper is organized as follows. First, we summarize the base constructs for a discussion on healthcare privacy in the United States. Then, we describe our survey of actual privacy policies used by healthcare organizations and assess them. This is followed by a description of infrastructure for privacy protection that is based on this notion of policy refinement, which enables improved privacy practices in healthcare. Finally, we conclude with a synopsis of the insight gained from this work.

BACKGROUND

Several data protection regulations have surfaced around the globe (Wong, 2009) over the last few decades that directly impact healthcare privacy. Among these are the Personal Information Protec-