Chapter 7.7
Electronic Medical Records, HIPAA, and Patient Privacy

Jingquan Li
Texas A&M University-Kingsville, USA

Michael J. Shaw
University of Illinois at Urbana-Champaign, USA

ABSTRACT

The continued growth of healthcare information systems (HCIS) promises to improve quality of care, lower costs, and streamline the entire healthcare system. But the resulting dependence on electronic medical records (EMRs) has also kindled patient concern about who has access to sensitive medical records. Healthcare organizations are obliged to protect patient records under HIPAA. The purpose of this study is to develop a formal privacy policy to protect the privacy and security of EMRs. This article describes the impact of EMRs and HIPAA on patient privacy in healthcare. It proposes access control and audit log policies to safeguard patient privacy. To illustrate the best practices in the healthcare industry, this article presents the case of the University of Texas M. D. Anderson Cancer Center. The case demonstrates that it is critical for a healthcare organization to have a privacy policy.

INTRODUCTION

The strategic utilization of information systems/information technologies (IS/IT) has played a central role in enabling organizations across many industry segments to address many business challenges and achieve a level of sustainable competitive advantage (Croasdell, 2001; Hammond, 2001; Holt, Love, & Li, 2000). Healthcare is noted for embracing new scientific discoveries and using leading edge technologies to enable better cures for diseases and better means to enable early detection of most life threatening diseases. Ironically, the healthcare industry in the United States, which has a greater need for more accurate and timely information, has experienced less development of IS/IT than other industries such as banks or airlines. The Health Insurance Portability and Accountability Act (HIPAA) of 1996 is the largest governmental law in healthcare since Medicare. HIPAA mandates new federal standards for elec-

tronic transactions, such as payment processing, patient's medical information privacy, and security procedures that secure the privacy protections. Currently healthcare organizations are contending with relentless pressures not only to implement IS/IT technologies but also to become compliant with HIPAA.

The growing use of healthcare information systems (HCIS) has provided healthcare organizations with tremendous benefits, including significantly reduced costs, reduced harmful medical errors, and improved quality of care. But the resulting dependence on electronic medical records (EMRs) has also kindled patient concern about patient data privacy and security. EMRs often contain some of the most sensitive information about who and what we are, such as mental and physical illness. Perhaps more than any other type of data, the confidentiality of EMRs is absolutely essential. When doctors' file cabinets held the bulk of medical records, the employees working in those practices had access to them. As hospitals and clinics switch to electronic record keeping, however, many more people might have access to private medical records. Under HIPAA, new healthcare privacy provisions designed to protect data transmitted and stored electronically went into effect April 14, 2003. The requirements of HIPAA and compliance issues are getting the attention of top executives in the healthcare industry.

Having a formal privacy policy is a key step in implementing any HIPAA compliance program. It should expressly cover how a health organization is protecting EMRs; the rules and limits on who can access and use EMRs; and the capability to track who has disclosed sensitive data and the circumstances of disclosure. A positive, formal, and continually practiced privacy policy by all employees can establish rules and limits on who can access and disclose EMRs and thus minimize the possibilities of privacy breaches. On the other hand, a poorly defined and improperly implemented and managed privacy policy can make EMRs ripe for privacy abuse. The HIPAA privacy rule puts an emphasis on access control and audit trails to protect patient data. This study investigates the use of access control and audit log policies to safeguard patient privacy.

The objective of this study is to develop formal access control and audit policies to protect the privacy of EMRs. The development of HIPAA compliance program and security policies has been addressed by several studies (Kieke, 2003; Messmer, 2003; DeMuro & Grant, 2001; Li & Shaw, 2004; Patient privacy, 2001). There are also several papers addressing the issue of protection of EMRs (Ateniese & Medeiros, 2002; Swartz, 2004). The closely related works to this study include the following. Zunkel (2005) studied how to use biometric technology to protect personal information and found that biometric technology does not endanger personal information; it protects it. Borrowing the principles of reporting and auditing from the accounting sector, Stevens (2002) found that through comprehensive reports of network activity logs and regular auditing of security measures and devices, healthcare organizations can generate the proof of HIPAA compliance. While these studies are devoted to technical aspects and particular access control and audit log technologies, this study takes a management-oriented approach to develop access control and audit log policies to protect EMRs strategically.

The rest of the article is organized as follows. In the second section, we discuss the issue of patient privacy in healthcare. In the third section, we describe the HIPAA privacy rule and its privacy implications. In the fourth section, we investigate access control and audit log policies to protect patient privacy. To illustrate the impact of EMRs on patient privacy and the importance of having a privacy policy in the healthcare system, we present a case example of the University of Texas M. D. Anderson Cancer Center in the fifth section. We conclude with a summary in the final section.