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.

Keywords: access control; case study; electronic medical record; medical record confidentiality; privacy protection; privacy regulations
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 expressively 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 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.

Patient Privacy in Healthcare

Traditionally, our medical records were kept in paper documents in different doctor’s offices. Cumbersome paper records not only contain too many errors and inefficiencies but also hinder communication between healthcare providers. According to the Journal of the American Medical Association, each year, as many as 98,000 patients die in U.S. hospitals from preventable medical errors, such as receiving the wrong medication. Nearly half of all patients do not get all the treatments or tests that they should have received. These problems persist because

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.
8 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the product’s webpage:

www.igi-global.com/article/electronic-medical-records-hipaa-patient/2486?camid=4v1


www.igi-global.com/e-resources/library-recommendation/?id=2

Related Content

A Survey of Attacks in the Web Services World
www.igi-global.com/chapter/survey-attacks-web-services-world/40593?camid=4v1a

Risk Analysis Using Earned Value: An Engineering Project Management Study
www.igi-global.com/article/risk-analysis-using-earned-value/133545?camid=4v1a

Investigating the Concept of Information Security Culture
www.igi-global.com/chapter/investigating-concept-information-security-culture/63080?camid=4v1a
Using Statistical Texture Analysis for Medical Image Tamper Proofing
www.igi-global.com/article/using-statistical-texture-analysis-medical/2484?camid=4v1a