Category: Concepts, Trends, and Challenges

Information Assurance in E-Healthcare

Sherrie D. Cannoy
The University of North Carolina at Greensboro, USA

A. F. Salam
The University of North Carolina at Greensboro, USA

INTRODUCTION

There is growing concern that the healthcare industry has not adopted IT systems as widely and effectively as other industries. Healthcare technological advances generally emerge from the clinical and medical areas rather than clerical and administrative. The healthcare industry is perceived to be 10 to 15 years behind other industries in its use of information technology (Raghupathi & Tan, 1997). Incorporating new technology into the healthcare organization's processes is risky because of the potential for patient information being disclosed. The purpose of this study is to investigate the information assurance factors involved with security regulations and electronic medical record initiatives—a first necessary step in making the healthcare industry more efficient. Noncompliance of a healthcare organization's employees with security and privacy policies (i.e., information assurance) can result in legal and financial difficulties, as well as irreparable damage to an organization's reputation. To implement electronic medical initiatives, it is vital that an organization has compliance with security and privacy policies.

E-health technology is a relatively current phenomenon. There are two types of distance-related healthcare that are technology driven. Telehealth is known for involving telemedicine—medicine practiced over a distance, with the impetus of control being in the physician's hands (Maheu, 2000). E-health involves the patient or physician actively searching for information or a service, usually via the Internet (Maheu). Electronic medical records fall into the e-health category because the physician, healthcare partners, and patient would be able to access the information through an Internet connection.

Security and information assurance are critical factors in implementing e-health technologies. There is a lack of a well-developed theoretical framework in which to understand information assurance factors in e-healthcare. The theory of reasoned action (TRA) and technology acceptance model (TAM) enable a conceptual model of information assurance and compliance to be formed in the context of healthcare security and privacy policy. The relationship between behavior and intentions, attitudes, beliefs, and external factors has been supported in previous research and will provide a framework for ensuring compliance to security and privacy policies in healthcare organizations so that HIPAA (Health Insurance Portability and Accountability Act) regulations are enforced and electronic medical records (EMRs) can be securely implemented.

Traditionally, records in the healthcare industry have been paper based, enabling strict accessibility to records. This allowed for confidentiality of information to be practically ensured. The uniqueness of healthcare records and the sensitive information they contain is specific to the industry. Over the many years that medical records have been kept, those involved in the field have undertaken a self-imposed rule of stringently protecting the patient information while providing quality care.

The patient's expectation for confidentiality of personally identifiable medical records is also critical. According to Rindfleisch (1997, pp. 95-96), in his study of healthcare IT privacy, the threats to patient information confidentiality are inside the patient-care institution; from within secondary user settings which may exploit data; or from outsider intrusion into medical information. Rindfleisch (1997) examined specific disclosures which could release sensitive information such as emotional problems, fertility and abortions, sexually transmitted diseases, substance abuse, genetic predispositions to disease—all of which could cause embarrassment and could affect insurability, child custody cases, and employment.

The process of healthcare treatment includes not only the patient and physician but also nurses, office staff who send out bills and insurance claims, the insurance company, billing clearinghouses, pharmacies, and any other companies to which these processes can be outsourced. There is an estimate that states as many as 400 people may have access to your personal medical information throughout the typical care process (Mercuri, 2004). The government is also a partner in national health concerns, and also maintains databases containing information on contagious diseases, cancer registries, organ donations, and other healthcare information of national interest. (See http://www.fedstats.gov/programs/health.html for a listing of the databases.)

With the advent of government mandates such as EMRs and HIPAA regulations, the increased accessibility of sensitive records requires intense effort to create policies that limit access for those who are authorized. Although there is an area of information economics which views information as an asset that can be numerically valued for its benefit, the same perspective has not been adopted in healthcare. Especially in the United States, clinical information and patient care are considered proprietary (Hagland, 2004). There is no specific associated cost with one's medical information—what damage is done when one's medical information has been utilized improperly? Even though damages are ill-defined, there are regulations and standards for emerging technology in healthcare. The two most current important security and privacy issues involve HIPAA regulation and the government mandate for EMRs.

BACKGROUND

The HIPAA Regulation . . .

HIPAA was enacted in 1996 and covers insurance reform for ensuring preexisting coverage when changing jobs as well as the standardization of electronic transmissions. It consists of two components, the Security Rule and the Privacy Rule. If the rules are not enacted, there are severe financial penalties enforced by the government (Mercuri, 2004). Also, an organization risks having internal employees disclose information that would be of a confidential nature to patients, which could result in legal consequences.

The Privacy Rule (Markus, 2004) focuses on the use and disclosure of medical information, specifically that which is personally identifiable, also known as protected health information (PHI) in the industry. The goal of the Privacy Rule is to ensure protection of PHI across transmissions to health partners (insurance companies, billing clearinghouses, etc.). This requires the patient to fill out the Notice of Privacy Practices Patient Acknowledgment form, which suggests that the patient has read the HIPAA privacy information and allows the patient to determine the people to which one's PHI can be disclosed.

The Security Rule requires that PHI be protected specifically in electronic storage and transmissions. Implications for HIPAA compliance have been intense. Developing standards and security encryptions for existing software, as well as ensuring that third-party partners are compliant, has been time-consuming and costly. However, Privacy and Security Rule compliance will be critical for successful implementation of electronic medical record infrastructure.

Electronic Medical Records

An electronic medical record (EMR) contains a patient's medical history with a physician. The capture of one's medical information can be made available to authorized users such as other physicians, pharmacists, insurance companies, and the government. Due to the inherent virtualization of the record, the physician's office or hospital will not have physical control as they have in the past. Therefore, security measures, mainly technical components, are critical to EMR implementation. EMR records will also fall under the HIPAA Privacy and Security Rules. Since the healthcare industry has been reluctant to implement EMR plans for cost, security, or other reasons, the government has taken an active role to encourage development of EMRs through financial incentives. Healthcare and IT organizations are also collaborating to develop standards (Mercuri, 2004).

Measures Needed for Better Management

Handling of sensitive information will be vital to understanding the compliance for HIPAA regulation, as well as for the implementation of EMRs. With information now being stored and transmitted electronically, a new paradigm exists for power over the information. How organizations measure the success of HIPAA compliance will reflect on how sensitive information is handled. However, it is uncertain how the healthcare industry monitors this. The old adage of "what is not measured is not managed" comes to mind and one wonders if compliance will be monitored after training is administered and policies are implemented. The purpose of this study is to develop a preliminary framework of issues that determine compliance to information assurance and security policies.

Information Assurance

Figure 1 (from Maconachy, Schou, Ragsdale, & Welch, 2001) in which the aspects of information assurance are depicted. They discuss information assurance as an expansion of the "coverage, responsibilities, and accountability of security professionals" which includes "proactive offensive activities" (p. 307).

Aspects of security services, information, and security countermeasures fall under the information assurance (IA) umbrella. The focus of IA is integrating the relationships between these, since a weakness in one would result in a weakness in the entire system. The information can be either currently in storage, in processing, or in transmission mode. The Security Services are carried not only by technological details such as availability of the system,