Adoption of Security Measures While Implementing Electronic Health Records

Barbara Hewitt

Texas A&M Kingsville System Canter San Antonio
1450 Gillette
San Antonio, TX 78224
Phone: (210)-932-6236 Fax: (210)932-6245
barbara.hewitt@tamuk.edu

ABSTRACT

For the past 50 years, security has been an issue for computer specialists. However, the potential security risks changed from less critical breaches such as someone stealing a few CPU cycles or performing computer pranks (Williams 2002) to extremely damaging issues such as identity theft, credit card theft, denial of service, or destruction of computer files and content. Healthcare organizations are struggling as one of the latest and last computer frontiers. Healthcare organizations are facing many issues including security issues while exploring the adoption of electronic health record (EHR) systems. This article proposes that while healthcare organizations should address authentication and access issues using biometrics and single sign-on (SSO) systems, many healthcare organizations are slow to adopt an EHR and slower to adopt biometric technology and single sign-on functionality despite the benefits of each.

INTRODUCTION

The Health Insurance Portability and Accountability Act (HIPAA) mandated the authority to regulate privacy of individually identifiable health information through the Standards for Privacy of Individually Identifiable Health Information (PIHI) (HIPAA 1996; PIHI 2001; Gunter and Terry 2005). President George Bush issued a directive that healthcare organizations implement EHR for most Americans by 2014 in Executive Order 13335 on April 27, 2004 (Horowitz, Mon, Bernstein, and Bell 2008). The rate of adoption for this initiative is currently still low. Just over 50% of large physician groups are using EHR (Lohr 2008). In a recent study of 2758 physicians, only four percent of physicians surveyed had a fully functional electronic record system and 13% reported having a basic system (DesRoches, Campbell, Rao , Donelan, Ferris, Jha, Kaushal, Levy, Rosenbaum, Shields, and Blumenthal 2008). The reasons that physicians are not adopting healthcare systems include economic constraints (66%), available systems did not meet their needs (54%), fear they would not see a return for their investment (50%), and fear the system would become obsolete (44%) (DesRoches et al. 2008). The reasons that hospitals cited for not adopting EHR systems were software costs (73%), hardware costs (66%), and lack of participation by physicians (59%) (Thakkar and Davis 2006). Many healthcare providers and organizations state that system costs are the biggest obstacle to the adoption of new systems (Thakkar and Davis 2006; DesRoches et al. 2008); however, the potential savings of effective EHR implementations with networking would be approximately $81 billion annually (Hillestad 2005).

While this initiative would improve healthcare efficiency and safety by enabling management of chronic disease and reducing duplication of tests and procedures, the potential costs associated with the advent of electronic records include securing the information stored in an EHR system. Healthcare organizations must ensure the privacy and security of patient data (Runy 2008). Examples of healthcare breaches include the accidental attachment of a document containing the names and addresses of HIV/AIDS patients to a personal email message, the theft of laptops from state health department employee's car and a Veteran Affairs employee's car, and disclosure of patient records such as when a staff member looked up acquaintances in an AIDS database and others who have looked up celebrities healthcare records (Myers, Frieden, Bherwani, and Henning 2008; Runy 2008).

Another major problem is medical identity theft. Medical identity theft occurs when an individual without medical insurance steals the identity of an insured individual and impersonates the insured individual in order to receive medical services such as surgery or drugs (Andrews 2008). In this type of identity theft, the uninsured individual's medical record can be incorporated into or replace the insured's medical record causing major medical issues and risk to the rightful owner of the medical record. Medical identity theft also occurs when fraudulent claims are filed to bilk Medicare, Medicaid, and insurance companies out of millions in false medical claims (Andrews 2008). In this type of theft, a healthcare provider files fraudulent healthcare claims to be reimbursed for procedures that were not performed on a patient. While some of these breaches were blatant misuses of confidential information, other breaches occurred due to employee negligence or carelessness.

Another issue that must be addressed is authentication when many individuals are using the same computer. While employees in most organizations have a single computer assigned for their use, in healthcare organizations, multiple individuals may access an EHR from a single computer. To address these issues, health care organizations must be able to authenticate multiple users on the same computer. It must allow these individuals access to confidential information from multiple systems on this shared computer. Though using usernames and passwords suffice for many organizations, healthcare organizations must overcome issues related to security and the use of these multiple systems simultaneously. Consequently authentication becomes more complicated.

Role based authentication controls (RBAC) could solve some of these issues in a less security oriented environment. However, individuals in a healthcare setting must be authenticated so that each individual only accesses information he is authorized to view or update. The EHR must also provide a proper audit trail to determine who accessed which patient record and what they did including any updates with date and time stamps. An EHR with proper authentication software can assist in solving these issues. This paper will explore what will increase the likelihood of a healthcare organization adopting an EHR, a biometric authentication system, and a single sign-on system.

LITERATURE REVIEW

This paper suggests that healthcare organizations should adopt biometrics for authentication purposes and use single sign-on systems when implementing EHR systems. This section explains

the needs for these methodologies. It concludes with the benefits these systems will provide health care organizations as well as identifying some technologies that may resolve these issues.

Most organizations including healthcare organizations use passwords for authentication. For most healthcare organizations, the first lines of defense between a patient's confidential information to affront privacy breaches is an employee's password (Medlin and Romaniello 2007). In a study of 90 healthcare workers, Medlin and Romanelli (2007) found that simple password cracking programs were able to crack 31% of the passwords in less than a minute. Half of the passwords used in one facility were cracked within one hour. The program cracked all but five passwords within 10 hours. Based on these findings, the authors recommended that organizations should implement a password policy. Employees should acknowledge the policy by signing it and attend training or education sessions. HIPAA regulations require similar efforts (HIPAA 1996).

While these suggestions for enforcing good password procedures will assist in securing EHR, healthcare organizations face additional challenges to securing medical records. First, many healthcare providers need to have access to multiple systems including radiology, pharmacy, clinical, surgical, and research (Ashmad and Rodriquez 2006). A healthcare provider's access to patient information must be instantaneous as found in a SSO system. A SSO system should allow individuals to quickly gain access to multiple different systems available for their use in treating patients. While some organizations such as Duke University Medical Center and Health System have implemented single sign-on (SSO) systems for the most critical applications, staff members from many organizations must sign on to each system that they need to access using a different password. A major problem that Duke found with its SSO system was that over 40% of the calls to the IT helpdesk was to aid healthcare providers who had forgotten their passwords (Ashmad and Rodriquez 2006).

Second, healthcare settings are dynamic, disruptive environments. During crisis, healthcare providers including physicians, nurses, radiologists, and technicians may have to leave workstations unattended quickly. Therefore, these systems must have short time-outs. However, when the healthcare provider returns to the terminal they may need instantaneous access to view pertinent information about a patient they are treating. Sometimes even the time it takes to enter a password is critical to the patient.

Third, although some healthcare facilities may have a computer available for each staff's usage, other facilities may have a couple of workstations within a care unit or on a floor that several staff must share. Each individual must be authenticated each time they access confidential patient information. Since healthcare providers may need to share devices within healthcare environment such as a nurse's station within a hospital, these systems should also allow multiple individuals to log on simultaneously also. Under these circumstances, each individual care provider must be able to log onto a computer that may already have other users. In order to share a device, each individual must remain logged in using his own authentication but his access should be automatically locked when he walks away from the computer. When an individual returns to the system, a simple procedure should authenticate the user and return him to his recent computer access. To share devices this way, additional software that will assist in the quick adjustment from one user to another should be incorporated into the new EHR system.

Fourth, the Privacy and Security Rules of the Health Insurance Portability and Accountability Act (HIPAA) offer guidance on securing patient records. Notably, much of the detail is left to the healthcare organizations' interpretation (Runy 2008). Runy (2008) noted that different regulations are specified for different types of healthcare organizations. However, all organizations are charged with the task of protecting electronic health records.

Fifth, patients receive service in multiple departments (Runy 2008) and often their care information is stored in different online and paper systems. Healthcare providers must view these records from different sources. Often access is created using a role-based approach. Regardless of what approach is used, each individual care giver must have access to a patient's information on a need to know basis. A healthcare provider should only see records of his or her patients and not other patient records. By authenticating each individual user, the system will know which records the provider needs to access.

Finally, some healthcare organizations are also using other options for authentication including smart cards, digital signatures, and biometrics (Krawczyk and Jain 2005; Andrews 2006). A problem with smartcards is that the card can be lost, stolen, copied or otherwise compromised. Krawczyk and Jain (2005) explored digital signatures (private key authentication) and voice modalities biometrics as a robust authentication method for physicians using tablet PCs. Sentillion's most extensive market of users for its fingerprint biometric technology are healthcare organizations (Andrews 2006). Some healthcare providers are bypassing fingerprint scanning and use handprints, retinal scans, face geometry, or dynamic signatures (Andrews 2006). St Vincent's Hospital and Healthcare Center is a network of eight hospitals and ancillary healthcare facilities in the Indianapolis area that implemented fingerprint scanners along with a single sign-on authentication method in 2001 (IndentiPHI 2007).

Fingerprint devices are sensitive to dirt, grime, grease, and cleaning solutions (Scott 2004; IndentiPHI 2007). The need to wear gloves as well as sterilization issues may also hinder using touch type devices. However, in other areas such as surgical suites and radiology, individuals must cover their faces with masks or shields. Thus while facial recognition or retinal scanners may be a better solution for some departments, voice recognition or fingerprint devices may be more applicable in others. Facial recognition, retinal scanners, and voice recognition devices are less intrusive and more sterile since there is no contact required between the user and the device. However, in some settings, these devices will not be conducive to patient care. Thus a multitude of biometric systems may need to be explored and incorporated into these systems.

Although adoption an EHR does not guarantee that the healthcare organization will adopt a SSO and/or a biometric device, healthcare providers may be more reticent to adopting EHR when the system does not contain an easy authentication method that allows the provider quick access to vital information about the patient for whom he/she is administrating care. The best solution would be an EHR that encompasses a single sign-on system, easily handles multiple users per station, and biometrics for authentication.

PROPOSED MODEL

To examine what factors influence the adoption of a biometric authentication and single sign-on system when adopting an EHR, this paper will explore the adoption process via a modified technology adoption model that was proposed by Wu and Wu (2005). Wu and Wu explored the adoption of customer relationship management systems by integrating aspects of Davis' (1989) technology acceptance model (TAM) with Roger's (1995) innovation diffusion theory (IDT). Their model includes factors to measure both IDT and TAM. The IDT factors include innovation, task, individual, organization, and environment. To measure innovation, they used relative advantage, compatibility, complexity, observability, and trialability using an instrument developed by Moore and Benbasat (1991). Kwon and Zmud's items were adapted to measure task, individual, organizational, and environmental factors. This model was proposed by Wu and Wu (2005) explored the adoption of customer relationship management systems by integrating aspects of Davis' (1989) TAM with Roger's (1995) innovation diffusion theory (IDT) as shown in Figure 1.

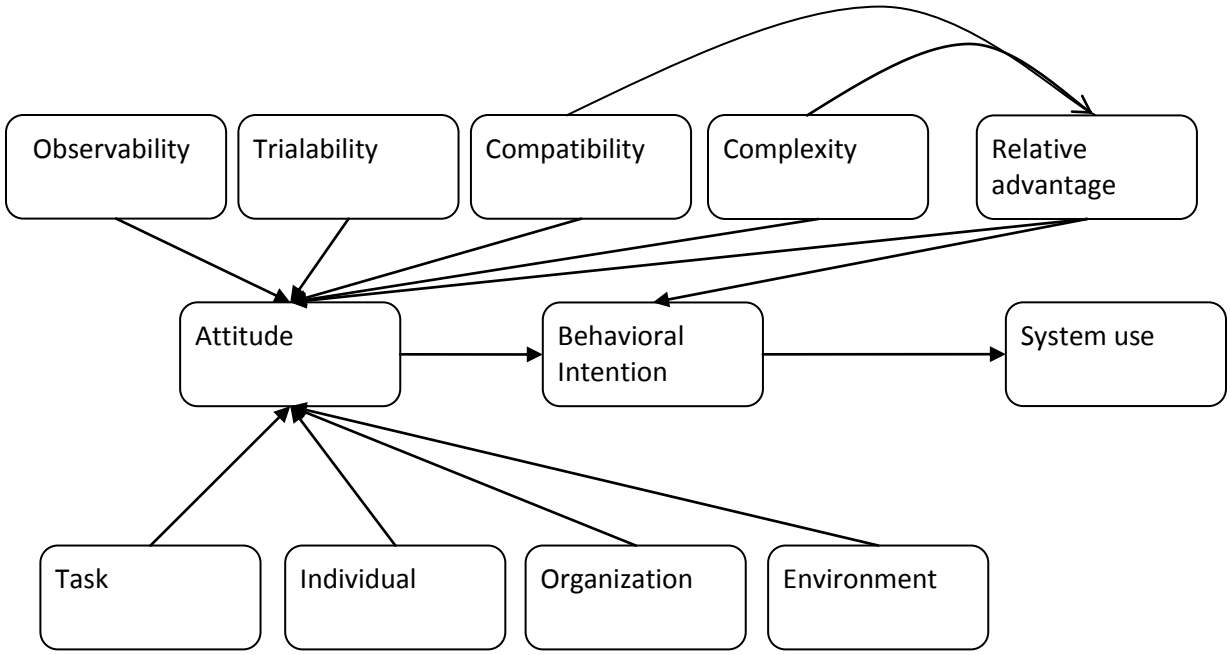

Figure 1. Wu and Wu (2005) Modified Technology Adoption Model

While Wu and Wu did not include costs as a factor within their model, this research proposes that cost should be included as a factor within the modified TAM model since most prior studies found that healthcare organizations were slow to adopt EHR due to the costs associated with implementing these systems. Security is another factor that has played a role in EHR adoption. This research proposes using a modified technology adoption model (TAM) to explore why healthcare organizations are slow to adopt EHR with biometric technologies and single sign-on as shown in Figure 2.

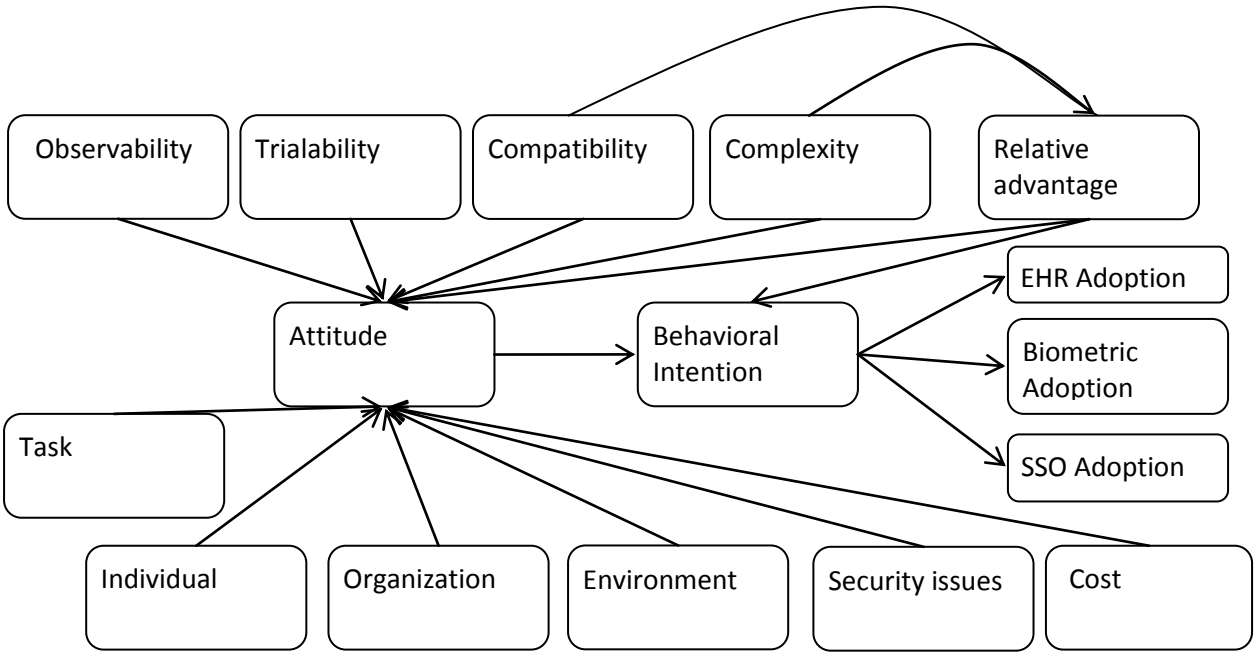

Figure 2. Proposed SSO and Biometric Adoption Model

METHODOLOGY

This research will use a field survey to test the proposed model. The survey will use items that Wu and Wu (2005) included in their study. A pilot study will be used to test the reliability and validity of the survey since additional items for cost and security must be incorporated into the questionnaire. The pilot study will be administered to a group of healthcare administration students at a major university.

The researcher will contact the Health Information Management System Society (HIMSS) to identify Chief Information Officer (CIOs) of healthcare organizations. These CIOs will be asked to respond to the survey. The survey will be offered online or via a paper document.

While many conventional statistical analysis procedures such as ANOVA, linear regression, multiple regression analysis, and factorial analysis can be used to test the individual paths or hypotheses, researchers should use some type of path analysis methodology to analyze a model (Gefen, Straub Jr., and Boudreau 2000). This study will use partial least square (PLS) or structural equation modeling (SEM) to evaluate the model shown in Figure 2 depending upon sample size. PLS can be used for small sample sizes while SEM requires larger sample sizes (Chin 1997).

CONCLUSION

In the interest of meeting HIPAA regulations and Executive Order 13335, healthcare organizations are slowly adopting EHR systems. Healthcare organizations should include an authentication methodology that allows users to quickly gain access to a patient's EHR and to all electronically stored information about a patient once access is granted. The system should allow multiple users; however, each individual user should only be able to access the information that he or she is authorized to view.

Limitations

This research has many limitations. For example, the research will only explore organizations that are planning to adopt EHR systems; therefore, organizations who have already adopted any of these systems will not participate in this research.

This study does not explore the legal aspects or ramifications of SSO systems. While some healthcare organizations are implementing SSO systems, some states may have laws that prohibit such access that will need to be addressed prior to implementation of such systems. Another issue associated with single sign-on is that once the system is compromised the intruder has access to all systems. However, biometrics will make this breach more complicated though not impossible.

Due to the many constructs in the proposed model, the survey for this study will be long. Thus the survey will take a lengthy amount of time to complete. This will reduce the number of responses since most CIOs are too busy to answer extensive surveys.

Theoretical Implications

This research offers a theoretical approach to explore why more healthcare organizations have not adopted an EHR or security measures with the adoption of an EHR. This study will extend past works that explored adoption models such as TAM, IDT, and many modified TAM models to determine if factors external to these existing models such as cost and security are of interest to the healthcare environment.

Practical Implications

Healthcare organizations are slow to adopt an EHR with single sign-on and biometric technologies to be used in conjunction with these systems. This study will offer healthcare organizations insight into the dynamics of adopting EHR along with single sign-on and biometric technologies.

REFERENCES

Andrews, J. (2006). "Biometrics leaves imprint on healthcare." Healthcare IT News.

Andrews, M. (2008). "Medical identity theft turns patients into victims." US News.

Ashmad, A., and Rodriquez, R. (2006). "Best Practices: Duke identifies with security needs." Information Week.

Chin, W. W. (1997, October, 18). "Overview of the PLS method." Retrieved April 29, 2006, from http://disc-nt.cba.uh.edu/chin/PLSINTRO.HTM.

Davis, F. D. (1989). "Perceived usefulness, perceived ease of use, and end user acceptance of information technology." MIS Quarterly **13**: 318-339.

DesRoches, C., Campbell, E., G, Rao , S. R., Donelan, K., Ferris, T. G., Jha, A., Kaushal, R., Levy, D., Rosenbaum, S., Shields, A., and Blumenthal, D. (2008). "Electronic health records in ambulatory care -- A national survey of physicians." The New England Journal of Medicine **359**(1): 51-60.

Gefen, D., Straub Jr., D. W., and Boudreau, M.-C. (2000). "Structural Equation Modeling and Regression: Guidelines for Research Practice." Communications of the Association of Information Systems **4**(7): 1-77.

Gunter, T. D., and Terry, N. P. (2005). "The emergence of national electronic health record architectures in the United States and Australia: Models, Costs, and Questions." Journal of Medical Internet Research **7**(1).

HIPAA (1996). Health Insurance Portability and Accountability Act of 1996 (HIPAA). Pub.L. 104-191, Aug. 21, 1996, 110 Stat. 1936.

Horowitz, J., Mon, D., Bernstein, B., and Bell, K. (2008). Defining key health information technology terms. D. o. H. H. Services, Office of the National Coordinator for Health Information Technology.

IndentiPHI, I. (2007). "Biometric security for St. Vincent Hospital and Healthcare Centers." Retrieved Oct 23, 2008, from http://www.identiphi.net/datasheets/StVincentHealthcare_White%20Paper.pdf.

Krawczyk, S., and Jain, A. K. (2005). Securing electronic medical records using biometric authentication. Lector Notes in Computer Science. Berlin, Springer Berlin. **3546/2005:** 1110-1119.

Lohr, S. (2008). Most doctors aren't using electronic health records. New York Times. New York, New York Times Company.

Medlin, B. D., and Romaniello, A. (2007). "An investigative study: Health care workers as security threat suppliers." Journal of Information Privacy & Security **3**(1): 17.

Moore, G. C., and Benbasat, I. (1991). "Development of an Instrument to Measure the Perceptions of Adopting an Information Technology Innovation." Information Systems Research **2**(3): 192-222.

Myers, J., Frieden, T. R., Bherwani, K. M., and Henning, K. J. (2008). "Ethics in public health research: Privacy and public health at risk: Public health confidentiality in the digital age." American Journal of Public Health **98**(5): 793-801.

PIHI (2001). Standards for Privacy of Individually Identifiable Health Information (PIHI). Federal Register. **codified at 45 CFR §160, §164**.

Rogers, E. M. (1995). Diffusion of Innovation Theory. New York, Free Press.

Runy, L. A. (2008). "The best line of defense: Hospitals take a proactive approach to data security threats." Hospitals and Health Networks **7**(3): 22-26.

Scott, M. (2004). "Fingers point toward biometrics." For the Record **16**(16): 29.

Thakkar, M., and Davis, D. C. (2006). "Risks, barriers, benefits of EHR systems: A comparative study based on size of hospital." Perspectives in Health Information Management(5).

Williams, S., Ed. (2002). Free as in Freedom. Sebastopol, CA, O'Reilly & Associates, Inc.

Wu, I.-L., and Wu, K.-W. (2005). "A hybrid technology acceptance approach for exploring e-CRM adoption in organizations." Behaviour & Information Technology **24**(4): 303-316.