Information Security Principles for Electronic Medical Record (EMR) Systems

Mohammed Rahman
Information Systems and Cyber Security, University of Texas at San Antonio, San Antonio, TX, United States.,
mohammed.rahman@utsa.edu

Christopher Kreider
Department of Information Systems, University of Texas at San Antonio, San Antonio, TX, United States.,
Christopher.Kreider@utsa.edu

Information Security Principles for Electronic Medical Record (EMR) Systems

Mohammed Sajedur Rahman
University of Texas at San Antonio
mohammed.rahman@utsa.edu

Christopher Kreider
University of Texas at San Antonio
christopher.kreider@utsa.edu

ABSTRACT

A growing number of healthcare organizations are replacing their traditional record keeping methods with the electronic medical record (EMR) systems as part of an on-going effort toward the digitization of healthcare. With the growing use of this digital information system, concerns about the state of security for the EMR systems have also increased. In recent years, a large number of academic and non-academic research activities are directed toward the use and implementation of EMR, however, very few of these studies are focused on the issue of security within the EMR systems. This paper explores the basics of computer security and proposes security principles that should be considered as guidelines at the time of EMR systems implementations. Our analysis of the literature and theory provides new insight for researchers and assists healthcare practitioners with increased security for EMR adoption.

Keywords (Required)

Healthcare Information System, Hospital Security, Patients Security, Electronic Medical Record, EMR, EMR Security, Adoption, Hospital Information System.

INTRODUCTION

Digitization of medical records is widely accepted by the healthcare professionals as one of the many ways to reduce the cost while at the same time improving the quality of healthcare. The rate of EMR adoptions by healthcare facilities in the United States, and associated research, has peaked in the past few years. Despite this trend, very few of these studies have focused on the security issues and concerns associated with the EMR systems, a sentiment reflected in many areas of IS research (Zafar and Clark, 2009). EMR systems provide an unique landscape to explore security practices, as the power structure and the independence of physicians is uncharacteristic of the traditional system user, and a far cry from the military environments where most information security practices originated (Adams, Sasse, and Lunt, 1997; Lapointe and Rivard, 2005; Wilkes, 1991).

The purpose of this paper is to explore and propose information security principles that should be considered as guidelines at the time of EMR design and implementation. As a result, we make a call for the development of usable and transparent security that is capable of meeting the specialized needs and the unique challenges present in medical organizations.

Even though EMR is a relatively recent phenomena, we feel that continued exploration of adoption issues will strengthen the identity of the IS discipline through the exploration of salient issues and supporting the continued maintenance of the disciplines plasticity, two of the proposed drivers of academic legitimacy proposed by Lyytinen and King (2004). Specifically, by searching through the existing non-EMR security research, we provide a proposed adaptation to the needs of EMR systems, which we argue differ from the military and traditional organizations from which most accepted security practices originated.

The remainder of this paper is organized as follows. The next section presents an in-depth look into EMR systems by reviewing the extant literature. We then focus on the unique nature of EMR and how EMR systems differ from other healthcare systems. Finally, we will make the connection to computer security, focusing on the perceived security threats to EMR systems, and discuss the applicability of the security principles in the EMR systems to minimize those threats.

LITERATURE REVIEW

Hannan (1996) defined the Electronic Medical Record System (EMR) as "the storage of all health care data and information in electronic formats with the associated information processing and knowledge support tools necessary for the managing the health enterprise system". EMR systems are designed to serve a variety of actors in the healthcare industry including physicians, nurses, hospital administrators and, most importantly, patients (Lapointe and Rivard, 2005; Sprague, 2004). Healthcare providers, as the primary actors, can create, collect, store, manage, and exchange individuals' medical information electronically in digital formats. The EMR systems directly impact patients by improving patient safety, supporting patient care, managing chronic conditions, and improving hospitals efficiencies (Sprague, 2004).

EMR History:

As early as 1958, programs were being designed to store and retrieve patient records (Stead, 1989). In the early 1970's, improving patient care became a primary goal with the creation EMR systems (Hannan, 1996). One of the earliest successful implementation of EMR system was in 1976 where it was demonstrated that the use of computer based medical record system resulted in a reduction of physicians' errors in detecting life-threatening events (McDonald, 1976). In 1991, the Institute of Medicine identified the computer-based record systems as "an essential technology for healthcare" (Dick and Steen, 1991). In 1996, the Health Insurance Portability Act (HIPAA) directed the U.S. Department of Health and Human Services to establish national standards for EMR systems (HIPAA, 1996). In 2004, the United States President issued an executive order setting an ambitious ten year goal of implementing EMR systems nationwide and providing all citizens with access to their health records (Ford, Menachemi, and Phillips, 2006). Finally, in 2009, a five year, $50 billion Presidential initiative aimed to link doctors and hospitals through new information technology, a plan that offered incentives for healthcare providers who utilized certified systems. Today, EMR systems serve as a complete workflow system for healthcare professional incorporating many routine tasks such as electronic prescription submission, patient order entry, diagnostic test ordering, test data analysis, patient billing, instant messaging, and patient alerts (Miller and Sim, 2004).

EMR Benefits:

Hillestad et al. (2005) conducted an in-depth study on the benefits of using EMR systems by healthcare organizations. They found that in addition to the quality improvements, EMR adopted hospitals could save over $80 billion annually and other parties such as Medicare and private payers were also projected to receive about $23 billion and $31 billion of the potential savings per year respectively. Several other studies support overwhelming benefits of EMR that outweigh costs and risks (Harrison and Ramanujan, 2011; Miller, West, Brown, Sim, and Ganchoff, 2005; Miller and West, 2007).

EMR Adoptions:

Despite the widely known benefits and a number of active incentive programs, few healthcare practitioners are yet using EMR systems. According to National Center for Health Statistics (NCHS), the use of fully functional EMR systems has only reached to around 10% as of early 2010 (Hsiao, Hing, Socey, and Cai, 2010). Analyzing the recent trends of EMR adoption by healthcare practitioners, the most conservative estimate is that it will take until 2024 for around 87% of the physicians to adopt EMR systems (Ford et al., 2006). Although the rate of EMR adoption by the healthcare facilities is increasing, a recent National Research Council (NRC) committee found that "current efforts aimed at nationwide deployment of healthcare information technology will not be sufficient to achieve the vision of 21st century healthcare and may even set back the cause" (Stead and Lin, 2009).

Barriers to Adoption:

Although a significant number of studies (Harrison and Ramanujan, 2011; Hillestad et al., 2005; Miller and Sim, 2004; Miller et al., 2005; Miller and West, 2007; Sprague, 2004) suggest that the use of EMR systems could save billions of dollars every year, the rate of adoption is still quite low (Hsiao et al., 2010). The challenges healthcare organizations face when implementing EMR includes high initial costs, lack of funding, technological difficulties, lack of standards, difficulties with training and resistance to implementation/adoption by key stakeholders (Hoffmann, 2009; Lapointe and Rivard, 2005; Miller and Sim, 2004; Ossoff, Thomason, and Appleton, 2010; Shortliffe, 1999; Smith, Dinev, and Xu, 2011).

Usable Security

Research on information security has traditionally focused on the technical strength, with less attention on the weakest link, the user (Adams et al., 1997; Keith, Shao, and Steinbart, 2007). For example, the benefits of a strong password are nullified when a user, who not knowing any better, releases their secret phrase. At the root of this problem is the assumption that even a sophisticated a security system requires the user to use it properly. Despite a wide variety of research on user friendly alternatives, such options have not reached mainstream adoption (Kreider and Rao, 2010).

Even in the earliest days of information security, security practices and policies represented overheard for system users. The earliest practitioners of information security were those in rigid military environments, where it was safe to assume users could be forced to comply at the command of superiors, or be subject to harsh penalties (Adams et al., 1997; Wilkes, 1991). In organizations that exhibit this strong top down, authoritarian power structure, general deterrence theory predicts that the disincentives as the result of non-compliance will deter deviant acts (Straub, 1990). Environments where EMR systems are adopted exhibit a different user landscape and power structure, where physicians possess a far greater power of choice over what systems to use than the average user (Lapointe and Rivard, 2005). Furthermore, medical organizations differ in the fact the decisions made by physicians can result in the life or death of another human being, decisions that often need to be made in real time, and with the highest quality information. Imagine a physician who loses a smart card and/or forgets the password to a secure EMR system. Such a physician, needing critical access, could either go through proper channels and possibly endanger a patient's life, or circumvent proper security policies and practices by sharing passwords and/or smart cards.

Despite these major differences in medical organizations, the security practices implemented still leave the user as the weakest link. As a result, we expect that medical professionals will be more likely to circumvent EMR specific security artifacts and policies when convenient, thus increasing the role the user plays in reducing system security. As Keith, Shao, and Steinbart (2009) noted, when/if users decide not to comply with security policies perceived to be intrusive and counterproductive, overall system security will decline. Based on this, we argue that when developing security policies and practices for EMR systems, usable and transparent security practices should be preferred over those that are more intrusive, even if more technically sound.

SECURE EMR FRAMEWORK

Global EMR systems follow the trends set by e-commerce and financial industries by providing robust and ubiquitous services. Despite nearly a decade of industry wide efforts, system security still remains elusive. Even after significant, and well studied efforts (Hutchinson and Warren, 2003) to ensure total security of these systems, security breaches are still ongoing issues in the financial, banking, and e-commerce industries (Rotchanakitumnuai and Speece, 2003; Yenisey, Ozok, and Salvendy, 2005).

Based on several recent high profile incidents, the healthcare industry has proven vulnerable to lapses in security, resulting in large volume identity thefts. Given the nature of the healthcare industry and the amount of personal information available, the consequences of identity theft can be far worse than a similar act in the financial and banking industries (JSPC, 2007). Given that only 10-20% of healthcare facilities have adopted EMR, the healthcare industry has arguably not yet experienced the security issues to the same extent other industries have experienced. Based on the close relation to e-commerce and financial industries, we argue that as the adoption of EMR by the healthcare providers continues to grow, the concern about security and privacy will become an increasingly important issue. However, despite the wealth of research on EMR and security, very few of these studies are actually focused on EMR security, combining the two together, as well as on the issues and concerns associated with EMR systems.

To understand what sets EMR system security apart from traditional systems, a thorough understanding of how they differ both in terms of the specific security threats and counter-measures is necessary. This will help us to develop the appropriate security principles against those threats. To define and understand the concept of security in terms of healthcare, we turned to the US Department of Health and Human Services where security is defined as “the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability” (USDHHS, 2004). To define security attributes associated with EMR systems, Conklin (2009) derived computer security attributes from Landwehr (2001) which were authentication, accountability, audit ability, confidentiality, integrity, and availability. Conklin's analysis of these EMR security attributes occur at the system level, but had not been applied to a practical scenario.

Therefore, we have chosen to analyze the security threats associated with EMR systems and propose security principles that could be used to manage these threats. One unique nature of EMR systems is that, unlike other healthcare systems, EMR systems can be considered and categorized as encompassing the ensemble view of the IT artifact, where it is important to view the artifact as part of a computer system, and not just as an isolated artifact (Orlikowski and Iacono, 2001). Therefore most, if not all, of the threats associated with computer systems should also be applicable to the EMR systems. Drawing from past literature dealing with computer security and associated threats (ACR–SIIM, 2009; CMS, 2006; Einwechter, 2002; Landwehr, 2001; Rindfleisch, 1997), we have categorized the threats to EMR systems into two groups: Internal (insider) threats and External (outsider) threats.

Insider Threats

Insider threats are risks of intended damage on a system posed by an authorized user of that system. Traditionally, security practitioners devote most resources to external threats, but some consider insider abuse to be the greatest threat (Einwechter, 2002; Warkentin and Willison, 2009). Insider threats can be broken into three types: *Insider Curiosity, Insider Subornation, and Accidental Disclosures* (Rindfleisch, 1997). *Insider curiosity* is the abuse of access privileges by medical workers out of curiosity or for own purposes. A pharmacist misusing privilege to check others' medical history is considered as an act of insider curiosity. *Insider subornation* can be defined as intentionally accessing information and releasing to outsiders for spite, revenge or profit. *Accidental disclosure* arises in situations when medical personnel make innocent and un-intentional mistakes which may lead to disclosures of sensitive information, such as misplacing a laptop with patient records.

External Threats

External threats are risks of intended damage to a system posed by unauthorized user of that system. External threats to EMR, defined in HIPPA fall into three categories: *Threats to Confidentiality*, *Threats to Integrity*, *Threats to Availability* (ACR–SIIM, 2009; Barrows and Clayton, 1996; Bodin, Gordon, and Loeb, 2005; CMS, 2006). The threat to *confidentiality* occurs when sensitive information are made available to unauthorized personnel or processes (Hash, Bowen, Johnson, Smith, and Steinberg, 2008). Given the nature of private medical information and the trust patients have with their doctors, preservation of confidentiality should be a primary concern. Failure to protect confidentiality could result in a loss of trust between doctor and patient, potentially resulting in lower quality of treatment. Threats to *integrity* can be defined as threats by which data or sensitive information are altered or destroyed by in an unauthorized manner (Hash et al., 2008). Healthcare practitioners make life and death decisions and need access to the highest quality information. A patient's records that have been tampered with or destroyed in an unauthorized manner have the potential to detrimentally influence patient care. Threats to *availability* can be defined as any threat that hinders the accessibility and usability of sensitive information when demanded by authorized personnel (Hash et al., 2008). As medical organizations become increasingly reliant on the ability to monitor and perform tasks in real time, being denied legitimate access to the system has the potential to reduce the quality of patient care.

The threats to EMR systems should not only be considered in terms of threats to the system, but also by how a violation would potentially affect patient care. In the next section, we will discuss and propose the security principles that could be used to minimize these threats to EMR systems.

PROTECTION MECHANISMS

In recent years, a number of incidents have been reported where patients' identities were compromised and medical information was fraudulently used to obtain prescription drugs (Andrews, 2008). With the increased use of EMR systems by healthcare providers the number of fraudulently use of medical information is also expected to increase (Alexander, 2006). The Health Insurance Portability and Accountability Act (HIPAA) developed and specified a set of privacy and security laws and regulations against these threats. However, as stated by Conklin (2009), "these regulations specify responsibility for protecting the information but do not specify how to achieve this protection".

EMR systems are used by many different actors such as doctors, nurses, lab technicians, administrators, and data entry workers, with many different levels of responsibility and workloads. Security policies or processes intended to increase security at the cost of patient care should be carefully scrutinized. Specific practices and policies deemed appropriate within the healthcare providers' workflow should be designed and implemented in such a way that the risk of direct impact on patient care is minimized. Again viewing EMR through the ensemble view of technology, we start with the general computer security principles and practices presented by Landwehr (2001).

Accountability

Accountability is the state of being accountable, liable, or answerable. Accountability is implemented through identification, authentication, authorization and auditing (Bhargav-Spantzel, Squicciarini, and Bertino, 2006; Landwehr, 2001). Identification asks a user who they are, authentication verifies their claim, authorization verifies what they can do, and auditing keeps track of what they have done (Bhargav-Spantzel et al., 2006; Evans Jr, Kantrowitz, and Weiss, 1974; Hovav and Berger, 2009). Implementing the accountability security principle within EMR systems, it is possible to minimize the insider threats of curiosity, subornation, and accidental disclosure by the authorized users of the systems. Accountability mechanisms represent an area where current technologies may not be sufficient to meet medical organizations specialized needs. Traditionally, accountability mechanisms have not been held in the highest regard by users and administrators alike, due to both the excessive burden placed on the user, and the ease with which users can circumvent a technically strong system (Furnell, 2005; Keith et al., 2009).

Least Privilege

Given the large number of EMR system users, and the wide variety of information and services available, EMR users should be granted the least level of access necessary (Saltzer and Schroeder, 1975). Furthermore, due to disparities in user responsibilities, least privilege is of critical importance to maintaining integrity of functionalities such as electronic prescriptions and test ordering. A least privilege security principles implemented at the process level should minimize the threats to availability, insider curiosity, and insider subornation threats.

Minimize the Complexity

As the level of effort required to establish trust is generally proportional to size and complexity, minimizing the complexities of the EMR system should minimize the risks of misuse and assurance cost. As medicine is one of the oldest disciplines, dealing with the complexities of human life, the design of a simple system may be somewhat idealistic. If oversimplification can result in lack of functionality, and excessive complexity can result in lack of security, a careful tradeoff should be made in the design of EMR systems. The complexity attribute must be implemented at the time of system design. An EMR system designed with an appropriate level of complexity, should help to reduce the threat to availability, and quality of patient care.

Default Security

From the onset, adequate security mechanisms and policies should be enabled by default for EMR systems. Default security should be applied in any situation where a threat could be preemptively mitigated, such as in the configuration of user accounts, and applications. By establishing default security, accidental oversights in the principal of least privilege should be minimized. The default security attribute should be at the time of system implementation and integration and should aim to reduce the threats to availability, confidentiality, and integrity of the system.

Defense in Depth

Any amount of efforts to ensure total security of a system may be inadequate. Given the constant and rapid changing nature of security, it is impossible for a system to exhibit total. Therefore, in order to deal with ongoing security threats, defense in depth is a best strategy to implement in information systems. EMR systems should be designed with multiple security features such as data classification, data encryption, strong security policies, and audit policies enforcement. Implementing defense in depth security feature will minimize the threats of unauthorized disclosure and disruption of healthcare information.

Regardless of the amount of security measures that are put in place within the system or within the processes, security breaches are expected. Therefore, in addition to the above security principles, number of additional steps can be taken in order to strengthen the security of EMR systems. Because of the unique nature of information security, Geer (2010) suggested to design information system with the aim of risk absorption rather than risk avoidance. Risk absorption of an information system can be ensured by implementing the following mechanisms.

Threats Category	Threats Types	Actions Lead to Threats	Protection Mechanisms
Internal Threats	Insider curiosity	Abuse or misuse of access privilege for curiosity	Accountability, Least Privilege
	Insider Subornation	Abuse or misuse of access privilege for revenge or profit	Accountability, Least Privilege
	Accidental Disclosures	Innocent mistake leading to unintentional disclosure	Accountability
External Threats	Threat to Confidentiality	Unauthorized access Unauthorized Use	Default Security, Defense in Depth
	Threat to Integrity	Unauthorized Disclosure Unauthorized Disruption	Default Security, Defense in Depth
	Threat to Availability	Unauthorized Modification Unauthorized Destruction	Least Privilege, Default Security, Minimize complexity

Table 1: EMR Security Threats and Protection Mechanisms

Detection and Monitoring

Adequate processes must be established to identify the incidents as well as to identify system and process flaws. Detection and monitoring capabilities should function as an alarm system and direct proper resources once the security incidence is detected. Detection and monitoring techniques should be designed to protect confidentiality of doctor patient privilege, and maintain the integrity of the healthcare organizations primary function.

Response and Recovery

The ability to respond and recover quickly to a security compromise can ensure minimal loss from both a technology, and patient care perspective. For EMR functionality that has the potential to directly influence patient care if compromised, appropriate alternative processes should be in place to ensure that the quality of care is not degraded. Once system service has been resumed, additional processes should be in place to quickly recover from the system down time, requiring minimal overhead for system users.

Continuous Improvement

Similar to other securities, information security is also a continuous process. Organizations must dedicate resources to follow the most up-to-dated technology trends. Organizational policies and processes must be updated as the technology and with it the security threats changes. On-going events must be closely monitored and key learning from every event must be logged and used to improve the current state of the systems.

CONCLUSION

With the increased use of EMR systems by the healthcare facilities, number of security threats targeting these systems and its information are also rapidly growing. Steps must be taken to ensure the safety and security of these systems. Securing information systems containing large amount of valuable public data can be a daunting tasks. Implementing the proposed security principles should minimize the security threats discussed in this paper. In addition to the security principles, steps must be taken to implement the risk absorption measures. Considering these security efforts may not guarantee a totally secured system but they will certainly minimize the threats to EMR systems' security.

REFERENCES

1. ACR–SIIM (2009) Practice Guideline for Electronic Medical Information Privacy and Security, A.C.o. Radiology.
2. Adams, A., Sasse, M. A., and Lunt, P. (1997) Making passwords secure and usable, *People and Computers*, 12, 1-20.
3. Alexander, M. (2006) Your Medical Recordso Stolen!, in: *Reader's Digest*.
4. Andrews, M. (2008) Medical identity theft turns patients into victims, in: *US News*.
5. Barrows, R. C. J., and Clayton, P. D. (1996) Privacy, confidentiality, and electronic medical records, *Journal of the American Medical Informatics Association*, 3, 2, 139-148.
6. Bhargav-Spantzel, A., Squicciarini, A. C., and Bertino, E. (2006) Establishing and protecting digital identity in federation systems, *Journal of Computer Security*, 14, 3, 269-300.
7. Bodin, L. D., Gordon, L. A., and Loeb, M. P. (2005) Evaluating information security investments using the analytic hierarchy process, *Communications of the ACM*, 48, 2, 78-83.
8. CMS (2006) CMS Policy for Information Security, Center for Medicare and Medicaid Services.
9. Conklin, W. A. (2009) Information Security Foundations for Electronic Medical Records, Americas Conference on Information Systems (AMCIS), San Francisco, California, pp. 1-6.
10. Dick, R. S., and Steen, E. B. (1991) The Computer-based Patient Record: An Essential Technology for Health Care, National Academy Press, Washington, D.C.
11. Einwechter, N. (2002) Preventing and detecting insider attacks using IDS, *SecurityFocus*, March, 1-7.
12. Evans Jr, A., Kantrowitz, W., and Weiss, E. (1974) A user authentication scheme not requiring secrecy in the computer, *Communications of the ACM*, 17, 8, 437-442.
13. Ford, E. W., Menachemi, N., and Phillips, M. T. (2006) Predicting the adoption of electronic health records by physicians: When will health care be paperless?, *Journal of the American Medical Informatics Association*, 13, 1, 106-112.
14. Furnell, S. (2005) Authenticating ourselves: will we ever escape the password?, *Network Security*, 2005, 3, 8-13.
15. Geer, D. E. (2010) Cybersecurity and National Policy, *Harvard National Security Journal*, 1, April 7, 2010, p^pp.
16. Hannan, T. J. (1996) Electronic medical records: An Overview, pp. 133-148.
17. Harrison, P., and Ramanujan, S. (2011) Electronic Medical Records: Great Idea Or Great Threat To Privacy?, *Review of Business Information Systems (RBIS)*, 15, 1, 1-7.
18. Hash, J., Bowen, P., Johnson, A., Smith, C., and Steinberg, D. (2008) An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule, NIST SP 800-66, U.S.D.o. Commerce, National Institute of Standards and Technology.
19. Hillestad, R., Bigelow, J., Bower, A., Girosi, F., Meili, R., Scoville, R., and Taylor, R. (2005) Can electronic medical record systems transform health care? Potential health benefits, savings, and costs, *Health Affairs*, 24, 5, 1103-1117.
20. HIPAA (1996) The Privacy Rule, HIPAA.
21. Hoffmann, L. (2009) Implementing electronic medical records, *Communications of the ACM*, 52, 11, 18-20.
22. Hovav, A., and Berger, R. (2009) Tutorial: Identity Management Systems and Secured Access Control, *Communications of the Association for Information Systems*, 25, 1, 531-570.
23. Hsiao, C. J., Hing, E., Socey, T. C., and Cai, B. (2010) Electronic Medical Record/Electronic Health Record Systems of Office-based Physicians: United States, 2009 and Preliminary 2010 State Estimates, *Hyattsville, MD, USA: National Center for Health Statitsics*.
24. Hutchinson, D., and Warren, M. (2003) Security for internet banking: a framework, *Logistics Information Management*, 16, 1, 64-73.
25. JSPC (2007) Information Security Risk Management for Healthcare Systems, NEMA/COCIR/JIRA Security and Privacy Committee (SPC).
26. Keith, M., Shao, B., and Steinbart, P. (2009) A Behavioral Analysis of Passphrase Design and Effectiveness, *Journal of the Association for Information Systems*, 10, 2, 63-89.
27. Keith, M., Shao, B., and Steinbart, P. J. (2007) The usability of passphrases for authentication: An empirical field study, *International journal of human-computer studies*, 65, 1, 17-28.
28. Kreider, C., and Rao, V. S. (2010) User Acceptance of Multiple Password Systems: A Proposed Study, Americas Conference on Information Systems, Lima, Peru.
29. Landwehr, C. E. (2001) Computer security, *International Journal of Information Security*, 1, 1, 3-13.
30. Lapointe, L., and Rivard, S. (2005) A Multilevel Model of Resistance to Information Technology Implementation, *MIS quarterly*, 29, 3, 461-491.
31. Lyytinen, K., and King, J. L. (2004) Nothing At The Center?: Academic Legitimacy in the Information Systems Field, *Journal of the Association for Information Systems*, 5, 6, 220-246.

32. McDonald, C. J. (1976) Protocol-based computer reminders, the quality of care and the non-perfectibility of man, *New England Journal of Medicine*, 295, 24, 1351-1355.
33. Miller, R. H., and Sim, I. (2004) Physicians' use of electronic medical records: barriers and solutions, *Health Affairs*, 23, 2, 116-126.
34. Miller, R. H., West, C., Brown, T. M., Sim, I., and Ganchoff, C. (2005) The value of electronic health records in solo or small group practices, *Health Affairs*, 24, 5, 1127-1137.
35. Miller, R. H., and West, C. E. (2007) The value of electronic health records in community health centers: policy implications, *Health Affairs*, 26, 1, 206-214.
36. Orlikowski, W. J., and Iacono, C. S. (2001) Research commentary: desperately seeking the" IT" in IT research-A call to theorizing the IT artifact, *Information Systems Research*, 12, 2, 121-134.
37. Ossoff, R. H., Thomason, C. D., and Appleton, J. (2010) Challenges with the Electronic Medical Record, *Journal of Health Care Compliance*, December, 51-54.
38. Rindfleisch, T. C. (1997) Privacy, information technology, and health care, *Communications of the ACM*, 40, 8, 92-100.
39. Rotchanakitumnuai, S., and Speece, M. (2003) Barriers to Internet banking adoption: a qualitative study among corporate customers in Thailand, *International Journal of Bank Marketing*, 21, 6/7, 312-323.
40. Saltzer, J. H., and Schroeder, M. D. (1975) The protection of information in computer systems, *Proceedings of the IEEE*, 63, 9, 1278-1308.
41. Shortliffe, E. H. (1999) The Evolution of Electronic Medical Records, *Academic Medicine*, 74, 4, 414-419.
42. Smith, H. J., Dinev, T., and Xu, H. (2011) Information Privacy Research: An Interdisciplinary Review, *MIS quarterly*, 35, 4, 989-1015.
43. Sprague, L. (2004) Electronic health records: How close? How far to go, *NHPF Issue Brief*, 800, 1-17.
44. Stead, W. (1989) A Quarter-century of Computer-based Medical Records, *MD Computing: Computers in Medical Practice*, 6, 2, 74-81.
45. Stead, W. W., and Lin, H. (2009) Computational technology for effective health care: immediate steps and strategic directions, The Nationall Academy Press, Washington, D.C.
46. Straub, D. W. (1990) Effective IS security, *Information Systems Research*, 1, 3, 255-276.
47. USDHHS (2004) HHS IRM Information Security Program Policy, HHS-IRM-2004-0002*,* U.S.D.o.H.a.H. Services.
48. Warkentin, M., and Willison, R. (2009) Behavioral and policy issues in information systems security: the insider threat, *European Journal of Information Systems*, 18, 2, 101-105.
49. Wilkes, M. V. (1991) Revisiting Computer Security in the Business World, *Communications of the ACM*, 34, 8, 19-21.
50. Yenisey, M. M., Ozok, A. A., and Salvendy, G. (2005) Perceived security determinants in e-commerce among Turkish university students, *Behaviour & Information Technology*, 24, 4, 259-274.
51. Zafar, H., and Clark, J. G. (2009) Current State of Information Security Research In IS, *Communications of the Association for Information Systems*, 24, 1, 571-596.