View metadata, citation and similar papers at core.ac.uk

brought to you by CORE

provided by AIS Electronic Library (AISeL)

Association for Information Systems
AIS Electronic Library (AISeL)

SAIS 2008 Proceedings

Southern (SAIS)

3-1-2008

Electronic Medical Record (EMR) Informatics Security

Byron Nicholson
Air Force Institute of Technology, Byron.Nicholson@afit.edu

Michael R. Grimaila
Air Force Institute of Technology

Dennis Strouble
Air Force Institute of Technology

Follow this and additional works at: http://aisel.aisnet.org/sais2008

Recommended Citation

Nicholson, Byron; Grimaila, Michael R.; and Strouble, Dennis, "Electronic Medical Record (EMR) Informatics Security" (2008). *SAIS 2008 Proceedings*. 27.
http://aisel.aisnet.org/sais2008/27

This material is brought to you by the Southern (SAIS) at AIS Electronic Library (AISeL). It has been accepted for inclusion in SAIS 2008 Proceedings by an authorized administrator of AIS Electronic Library (AISeL). For more information, please contact elibrary@aisnet.org.

ELECTRONIC MEDICAL RECORD (EMR) INFORMATICS SECURITY

Byron Nicholson
Air Force Institute of Technology
Byron.Nicholson@afit.edu

Michael R. Grimaila
Center for Cyberspace Research
Air Force Institute of Technology
Michael.Grimaila@afit.edu

Dennis Strouble
Center for Cyberspace Research
Air Force Institute of Technology
Dennis.Strouble@afit.edu

ABSTRACT

Medical records, once archived on paper and stored in filing cabinets, are now housed in electronic data repositories. While converting medical information into electronic format yields enormous benefits, it also raises new privacy and security concerns. The fact that medical information is now accessed, stored, processed, and transmitted through multiple organizations has led to the need for medical informatics security. In this paper, we examine the evolution of electronic medical records, review relevant legislation, and examine issues of privacy and security as it relates to medical information.

Keywords

Electronic medical records, medical informatics security, information security

INTRODUCTION

Today, Information Technology (IT) is utilized in virtually every organization as a means to increase productivity, reduce costs, and minimize delays when sharing information. While the management of information systems (MIS) discipline initially struggled to assert its legitimacy (King & Lyytien, 2004), it has proven invaluable to effectively plan and organize company information architectures. Arguably, a fraction of this success can be attributed to the relatively inexpensive cost of purchasing an Information System (IS) considering cost, at one time, was a technology barrier (Parente & Prescott, 1994; Anonymous, 2007). However, economical savings and budgetary windfalls produced by IT are often mitigated by the costs incurred to train personnel as well as implement and sustain (i.e., secure and update) IT systems. The capricious IS culture mandates robust MIS operations since the total cost of ownership has proven to be a baleful obstruction (Cavolo, 2007). Regardless of cost, IT and IS have created a societal dependence on their functionalities.

Before the mainstream use of IT, individuals' daily tasks were not filled with e-mails or other electronic distractions (i.e., instant messages). A momentary IT outage renders most organizations idle since a large part of their daily operations require IT resources to function efficiently. Many organizations' leadership has come to view IT as a valued resource whose implementation is necessary for its competition and success (Galliers & Leidner, 2004). Unfortunately, the moment a resource becomes a necessity is the exact same moment it becomes vulnerability. Senior leadership and top-management's attitudes towards technology systems often determine the level of organizational performance. Within the medical community, hospital administrators and medical chief information officers (CIO) have begun implementing more IT systems to handle electronic medical records (EMR/HER) (Glaser, 2007). These healthcare facilities are required by federal law to protect personal health information and ensure patient privacy rights are not violated (Arzuaga, 2004). The use of IS and IT systems has proven that, when implemented and utilized correctly, it can enhance an organization's performance. To protect sensitive information, healthcare organizations need to ensure that stringent information security practices and regulations such as the Health Insurance Portability and Accountability Act (HIPAA) of 1996 are followed (Collmann & Cooper, 2007).

MEDICINE MEETS TECHNOLOGY

The medical field, for various reasons, did not follow the status quo of industry leaders regarding the implementation of technology and its resources (Krizner, 2006). According to Carr (2003) "a resource only provides a competitive advantage when it is scarce versus ubiquitous". That is to say, a medical institution would have a better advantage over its competitors if it alone possessed IT and used the technology unlike any other organization. Carr's argument is legitimate as it applies to the corporate business world; its generalizability does not capture the basis as to why the medical field did not readily implement technology into its business practices. Instituting change is hard; Instituting change that affects not only years of medical practice but the potential loss of life is even more difficult (Peterson, 2006). The medical culture is one of codified procedures and precise routine that create a necessary stability (Frisse, 1997). If a member perceives its value as a good fit, that member will strongly resist any efforts that seek to upset the equilibrium (Robbins, 2005). It can be argued that technology had a difficult start in medicine primarily because the personnel did not readily accept it (Chau & Hu, 2002a).

Since Ajzen and Fishbein (1980) developed the Theory of Reasoned Action (TRA), technology adoption research has been replicated numerous times with proven models attempting to predict or validate the use of IT (Bagozzi et al., 1992; Davis et al., 1989). In 2002, there were a scarce number of published studies relating to healthcare and technology acceptance (Chismar & Wiley-Patton, 2002). Today, several studies have been conducted specifically targeting technology acceptance within the medical profession (Chau & Hu, 2002b; Hu et al., 1999). Two of the more common reasons cited within technology acceptance research as to why a piece of technology falls into disuse were the amount of time it takes to learn the new system and the users' perceptions as to whether or not the technology actually assists or hinders them in accomplishing their tasks (Davis, 1989). "Practitioners have often regarded technology as costly, cumbersome, and offering little help for tasks at hand" (Goldschmidt, 2005). Despite barriers such as cost or technology acceptance, technology usage within the profession has increased. Once an institution that relied solely on time-tested methods and medicines to cure ailments and injuries, the field of medicine has completely revolutionized itself from a self-sufficient profession (years of independent trial and error) to one that has become technology-dependent (rapid sharing of abundant, codified knowledge).

THE MERGE (MEDICAL INFORMATICS)

Collecting Patient Care Orders

Within the medical community, there is a professional understanding or a de facto standard of practice that states, "if it's not written down, then it never happened." Anyone who has visited a medical facility might have noticed medical personnel gathering information for health history and insurance purposes (Gustin, 2007). A large majority of a physician and accompanying staffs' time is spent writing or capturing information that has occurred or needs to happen. Healthcare facilities are transitioning from pen and paper to electronic methodologies to capture patient history and issue care orders. Although a small percentage of U.S. hospitals actually possess fully integrated computerized patient order entry systems (CPOE), among those that do, the systems are used by nearly 90 percent of physicians (Ash et al., 2004) To provide physicians better information that supports their decision-making, collected patient-related information is now being placed in electronic medical records housed in healthcare subsystems and accessed electronically by individuals with the correct authorization (Sensmeier, 2006). Time once consumed writing or translating handwritten orders, coupled with malpractice lawsuits spurred by errors attributed to illegible handwriting, is driving a change toward a technological solution to collecting patient order entries (Edwards & Moczygemba, 2004). Once collected, these orders are added to the patient's complete history of care and become part of that patient's medical record.

Medical Records

Patients' medical histories are documented within their medical records which must follow them over the course of their lifetime (Gustin, 2007). Normally the record is a collection of individual sheets of patient care orders, contained within a folder or series of folders and stored in a filing cabinet within the records department. These records are tightly guarded and strict audit logs are kept to account for each and every time someone accesses a record. Previously, this was a rather manual process involving human-to-human interaction (Eichelberg, 2005). However, with the adoption of electronic records, a patient's entire medical history is recreated into a digital format and can be accessed remotely at a terminal by appropriate personnel sans human intervention. Although electronic records are becoming more popular, paper records have not been completely replaced (Stausberg et al., 2003). Although medical informatics allow physicians to perform tasks faster, easier, and with less invasive methods to patients, the medical record must capture patient information regardless of format.

Introducing the Electronic Medical Record System

Electronic medical records, often referred to and used interchangeably with electronic health records (EHR) and computer-based patient records (CPR), are a hot topic and are increasing in popularity. The formal definition states that an EMR is "digitally stored health care information about an individual's lifetime with the purpose of supporting continuity of care, education and research, and ensuring confidentiality at all times" (Eichelberg, 2005). In many cases, it is the patients and not the medical professionals who are requesting electronic medical records. A national survey by Kaiser Permanente, the nation's largest non-profit organization, revealed that the majority of 1000 Americans surveyed would prefer physicians and insurance companies that use electronic medical records over those that do not (Swartz, 2007). The increased popularity of electronic medical records has also increased the number of health information exchanges (HIE) and regional health information organizations (RHIO) that operate within the country. The Health Information Management Systems Society (HIMSS) defines an RHIO as a "group of organizations with a business stake in improving the quality, safety, and efficiency of healthcare delivery” (Squazzo, 2007). In a rush to obtain EMR systems, many organizations are failing to acknowledge or understand the intricacies of operating such systems.

System Acquisition

Healthcare market trends indicate that more money is being allocated for medical informatics systems than ever before (Frisse, 1999; Krizner, 2006). In 2006, the Department of Defense (DoD) completed its nationwide rollout for its new EMR system Armed Forces Health Longitudinal Technology Application (AHLTA) and has mandated that all of its hospitals begin using the system. The DoD intends to maintain a continuity of care by ensuring that a service member’s record follows the individual for life. The change is part of a Pentagon-wide push to use electronic health records and eliminate a medical paper trail that requires service members to hand-carry their records to appointments and to permanent, overseas assignments (Swartz, 2006b). Software giant Microsoft has approached the DoD with hopes of managing all of its electronic medical records (Hookway, 2007). An achievement of this magnitude will depend largely on the innate ability of information technology to foster the exchange of electronic health information.

Although the comparative cost of individual IT systems has decreased, the total cost of ownership is a problem (Cavolo, 2007). Research indicates that the most effective barrier to EMR systems to date is the total cost of ownership. Aside from the budgetary constraints, another problem barring EMR success has little to do with actual system acquisition. The technology within these systems will continually evolve and require a robust change management strategy and system administration to ensure the information’s security and availability at all costs. Like all information technology, EMR systems facilitate the sharing of medical data and information. Considering patient privacy and risks associated with sharing this information, securing the networks that distribute this information is more important than the purchasing price.

Congress took legislative action in 2006 in attempts to boost e-health initiatives by re-addressing previous bills that supply health providers the grants necessary to implement health IT (Wechsler, 2007). However, even congressional assistance did not assuage the barriers to securing medical health IT. Medical organizations may possess the financial means to purchase the appropriate systems; however, that does not guarantee expected returns on their investments (Kaushal et al., 2006). Regardless of the hardships suffered obtaining or operating EMR systems, converting medical information into a digital or electronic format to circumvent physical limitations garners a host of new concerns for medical institutions regarding such areas as risk management as it pertains to patient privacy and information security.

SECURING THE ENTERPRISE

Health Insurance Portability and Accountability Act (HIPPA)

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) Title II outlines the provisions that organizations must take to ensure the privacy and security of a patient’s health information. Physically securing a folder containing a patient’s private medical history appears simple considering the folder is usually under lock and key and/or video surveillance; it is accessed by individuals with the right credentials (Arzuaga, 2004). Furthermore, there is the danger of information being physically removed, intentionally or maliciously, or even lost. HIPAA exists to ward off organizational complacency regarding the patient privacy information (Swartz, 2006a). Regardless, the paper folder is an entity that can only exist in one location at one time (barring duplications) where the physician, the nurse, or even the patient can physically see and touch it. This is not the case with the EMR where multiple entities of files can exist on several networked systems.

Medical Networks

The manner in which medical institutions utilize their “toll roads” upon the information superhighway is highly indicative of the changes IT has instituted throughout the field of medicine (Cimino, 1997). Today, medical personnel at geographically separated medical campuses share incredible amounts of information within mere seconds without ever physically touching it. Physicians and their staff members no longer need to be present to address the changing needs of patients. They are linked electronically to their work whether through E-mail, personal digital assistants (PDA), or video teleconferencing (VTC). This spans beyond any physical border and has shrunk the world. The increased usage of technology gives doctors, nurses, and hospital administrators access to critical and relevant clinical information as well as fostering communication amongst colleagues (Gates, 2007). The DoD, which is typically not near the forefront when it comes to implementing newer technologies, has recognized the importance of patient care and is taking necessary measures to ensure that its health care facilities follow the trend of its civilian compatriots and begin utilizing an EMR system. However, issues regarding storage, retrieval, and most paramount, information security risk are essential considering the amount and type of personal information captured in an electronic medical record.

The Federal Privacy Act of 1974 (5 USC sec. 552a) permits any civilian or patient-appointed individual access to their medical records. The sensitivity of the information contained with a patient's medical record requires a more stringent approach to ensure that information's security and availability which ultimately results in patient privacy. Table 1 summarizes a list of common security goals born from a collaborative effort between the United States, the European Council, and Canada in 1996 regarding information system security (Toyoda, 1998). The privacy and security of medical information is more than just a good idea or sound business principle; it is a law enforced by organizations such as HIPAA.

Common Information System Security Goals as defined by US, EC, Canada
a. System should be used by authorized security personnel
b. Security functions must protect against unauthorized alteration
c. User's actions must be logged
d. Data must be protected from changes or deletion
e. Data must be available whenever required
f. System must be managed using safe means
g. Action-related security must be made obligatory by the system operation

Table 1: System Security Goals

Before the digital era, threats to a patient's medical folder included any number of threats pertaining to paper products such as theft, corruption, water, fire, aging, etc. However, now that records are handled electronically, the same risks that applied to paper records apply to the EMR. Once sound security practices are instituted and adhered to, accessing a patient's medical history from any hospital only requires the proper identification and authorization

The Need for Standards

With large medical organizations adopting EMR systems, smaller institutions are forced to do the same. Here in lies a problem. Not all vendors are created equally nor do they provide the same functionality that would be compatible across platforms. Considering there are literally hundreds of software and hardware standards, it is impossible to avoid the inevitable situation of functional stove piping unless strict standards are established and enforced (Hooda et al., 2004). To combat the problem of inoperable EMR solutions, standards like the Health Level 7 (HL7) Clinical Document Architecture (CDA) and Integrating the Healthcare Enterprise (IHE) have been developed to structure and markup the clinical content for sharing amongst medical facilities and secondary users (Eichelberg, 2005). The ISO Technical Committee on Health Informatics describes its scope as "standardization" in the field of information for health, and Health Information and Communication Technology (ICT) to achieve compatibility and interoperability between independent systems (Eichelberg, 2005). Such standards mitigate the differences in vendors and contractors who provide IT support.

Most hospitals employ IT personnel who possess adequate knowledge pertaining to network administration. Their primary function, aside from network availability, is to ensure that any changes to the back-end of the network are transparent to the users (medical staff) (Hersh, 2006). However, with the adoption of new medical technology, it is far easier for hospitals to store their massive loads in off-site data warehouses. These warehouses are owned and operated by contractors who often subcontract other smaller companies to manage them. Aggregating staggering amounts of patient data in one location and then subjecting it to less-than-adequate security principles is unacceptable (May, 1998). Security personnel must be cognizant of information in their charge since a hole in security anywhere is a door to everywhere.

In January 2006, an orthopedic clinic in Fort Wayne, Indiana suffered an attack to its medical network. A hacker used a backdoor created after exploiting the clinic's MySQL database to access the system more than nine times over a two-week period (Vijayan, 2006). An FBI investigation discovered the hacker gained access via a proxy server at a nearby hospital connected to the orthopedic clinic's virtual private network (VPN). Once inside, the hacker created a hard-coded username and password to create the backdoor for future access. Incidents like these are not rare and stand as testimony to the dire need of robust security practices. Although many organizations are supplementing their security practices with such devices as smartcards or biometrics, these might not prove enough as medical identity theft and attacks become more sophisticated.

Just as industry and corporate businesses hire information specialists to secure their networks, so do medical institutions (Lafferty, 2007). However, unlike their corporate colleagues, medical institutions' chief information officers (CIOs) have an added measure that compounds their security practices; oftentimes, a disconnect exists between the medical technology and the specialists hired to secure it. Medical technology is often designed and managed by clinical engineers who may not understand the intricacies of data and information security. On the other hand, while the act of securing hospital medical data often falls to IT professionals, these professionals may not completely understand the clinical engineering world (Haugh, 2006). An ideal situation would include personnel knowledgeable in both arenas where they would be able to effectively design and manage medical informatics and networks. Unfortunately, there are no one-stop, security-in-a-box solutions to security despite most vendors' efforts to convince the unsuspecting that such products exists.

CONCLUSION

Securing a patient's medical record was indeed a manual and time-intensive endeavor when it was maintained in a folder filed away in a cabinet and required human-to-human interaction. The use of IT has removed that interaction in the auspice of facilitating easier access through the use of smartcards and biometric profiles; however, this access comes at a price. Without the proper security measures in place to protect patient health information, both the care provider and patient run the risk of having very sensitive information disclosed unintentionally. The conflict over who owns the medical record is an ongoing concern. HIPAA, Freedom of Information Act, or the Federal Privacy Act all dictate lucidly what role the patient and care providers play. However, the emergence of software that allows patients to access and store their records on personal computers is rewriting the rules (Lawton, 2007). However, it is the very nature of IT to promote easier exchange that poses a very real-time problem when it comes to securing a medical institution's information systems.

DISCLAIMER

The views expressed in this paper are those of the authors and do not reflect the official policy or position of the United States Air Force, the Department of Defense, or the U.S. Government.

REFERENCES

1. Ajzen, I. and Fishbein, M. (1980). Understanding Attitudes and Predicting Social Behavior, Prentice-Hall, Inc.
2. Anonymous, (2007). Hospital IT use growing strong. Trustee: The Journal for Hospital Governing Boards, 60(4), 4.
3. Arzuaga, P. (2004). HIPAA privacy rules: Protecting patient information requested through discovery, subpoenas and court orders. Employee benefits journal, 29(2), 28. 27.
4. Ash, J. S., Gorman, P. N., Seshadri, V., & Hersh, W. R. (2004). Computerized physician order entry in U.S. hospitals: Results of a 2002 survey. Journal of the American Medical Informatics Association, 11(2), 95-99.
5. Bagozzi, R. P., Davis, F. D., & Warshaw, P. R. (1992). Development and test of a theory of technological learning and usage. Human Relations, 45(7), 660-686.
6. Carr, N.G. (2003). "IT doesn't matter." Harvard Business Review.41-47.
7. Cavolo, D. J. (2007). Electronic medical record systems: Know the total cost of ownership. Nursing Homes, 56(7), 17.
8. Chau, P.Y.K., & Hu, P.J. (2002a). "Investigating healthcare professionals' decision to accept telemedicine technology: an empirical test of competing theories. (39) 297-311.
9. Chau, P.Y.K., & Hu, P. J. (2002b). Examining a model of information technology acceptance by individual professionals: An exploratory study. Journal of Management Information Systems, 18(4), 191.
10. Chismar, W.G., & Wiley-Patton, S. (2002). "Does the extended technology acceptance model apply to physicians," IEEE Proceedings of the 36th Hawaii International Conference on System Sciences.
11. Cimino, J. J. (1997). Beyond the superhighway: Exploiting the internet with medical informatics. Journal of the American Medical Informatics Association, 4(4), 279-284.
12. Collmann, J., & Cooper, T. (2007). Breaching the security of the kaiser permanente internet patient portal: The organizational foundations of information security. J. of the American Medical Informatics Association, 14(2), 239-243.
13. Davis, F. (1989). "Perceived usefulness, perceived ease of use, and user acceptance of information technology," MIS Quarterly. (13)3, 319-340.
14. Davis, F.D., Bagozzi, R., & Warshaw, P.R. (1989). "User acceptance of computer technology: A comparison of two theoretical models. Management Science, (35), 982-1002.
15. Edwards, M., & Moczygemba, J. (2004). Reducing medical errors through better documentation. The health care manager, 23(4), 329.
16. Eichelberg, M. (2005). A survey and analysis of electronic healthcare record standards. ACM Computing Surveys (CSUR), 37(4).

17. Frisse, M. (1997). IAIMS: Planning for change. Journal of the American Medical Informatics Association, 4(2), S13-19.
18. Frisse, M. C. (1999). The business value of health care information technology. Journal of the American Medical Informatics Association, 6(5), 361-367.
19. Galliers, R. D. & Leidner, D.E. (Eds.). (2004). Strategic information management. Butterworth-Heinemann Publishing.
20. Gates, B. (2007, Oct 5). Health care needs an internet revolution. Wall Street Journal, pp. A.17.
21. Glaser, J. (2007). The electronic health record: A digital divide? Healthcare Financial Management, 61(10), 38.
22. Goldschmidt, P.G. (2005) HIT and MIS: implications of health information technology and medical information systems, Communications of the ACM, v.48 n.10.
23. Gustin, G. (2007). The collection and recording of patient history in today's electronic world. Journal of Health Care Compliance, 9(4), 49.
24. Haugh, R. (2006). IT gets HIPAA. Hospitals & Health Networks, 80(9), 14.
25. Hersh, W. (2006). Who are the informaticians? what we know and should know. Journal of the American Medical Informatics Association, 13(2), 166-170.
26. Hooda, J. S., Dogdu, E., & Sunderraman, R. (2004). Health level-7 compliant clinical patient records system. Applied Computing 2004 - Proceedings of the 2004 ACM Symposium on Applied Computing, 259-263.
27. Hookway, J. (2007, Oct 30). Business technology: Microsoft to buy health software. Wall Street Journal, pp. B.4.
28. Hu, P. J., Chau, P. Y. K., Sheng, O. R. L., & Tam, K. Y. (1999). Examining the technology acceptance model using physician acceptance of telemedicine technology. Journal of Management Information Systems, 16(2), 91.
29. Kaushal, R., Jha, A. K., Franz, C., Glaser, J., Shetty, K. D., Jaggi, T., et al. (2006). Return on investment for a computerized physician order entry system. Journal of the American Medical Informatics Association, 13(3), 261-266.
30. King, J.L. & Lyytinen, K. (2004). “Reach and Grasp.” MIS Quarterly. (28)4, 539-551.
31. Krizner, K. (2006). Provider IT spending on the rise in north america. Managed Healthcare Executive, 16(2), 11.
32. Lafferty, L. (2007). Medical identity theft: The future threat of health care fraud is now. Journal of Health Care Compliance, 9(1), 11.
33. Lawton, C. (2007, Sep 4). New services help unsnarl medical bills; slew of online tools let consumers create and manage their own digital records; typing it in yourself. Wall Street Journal, pp. D.1.
34. May, T. T. (1998). Medical information security: The evolving challenge. Proceedings IEEE 32nd Annual 1998 International Carnahan Conference on Security Technology (Cat no 98CH36209) CCST-98, 85-92.
35. Parente, S. L., & Prescott, E. C. (1994). Barriers to technology adoption and development. The Journal of Political Economy, 102(2), 298.
36. Peterson, H. E. (2006). From punched cards to computerized patient records: A personal journey. IMIA Yearbook of Medical Informatics, 45, 180-186.
37. Robbins, S.P., & Judge, T.A. (2007). Organizational Behavior. New Jersey: Pearson Prentice Hall.
38. Sensmeier, J. (2006). “Survey says: Care, communication enhanced by IT”. Nursing Management, 2.
39. Squazzo, J. D. (2007). The state of regional health information organizations: Health data exchange on the rise. Healthcare Executive, 22(5), 8.
40. Stausberg, J., Koch, D., Ingenerf, J., & Betzler, M. (2003). Comparing paper-based with electronic patient records. Journal of the American Medical Informatics Association, 10(5), 470-477.
41. Swartz, N. (2006a). Government not enforcing HIPAA. Information Management Journal, 40(5), 20.
42. Swartz, N. (2006b). Pacific bases begin move to EMR system. Information Management Journal, 40(4), 13.
43. Swartz, N. (2007). Americans prefer electronic health records. Information Management Journal, 41(4), 8.
44. Toyoda, K. (1998). Standardization and security for the EMR. Intl. Journal of Medical Informatics, 48(1-3), 57-60.
45. Vijayan, J. (2006). FBI probes hacking incident at Indiana clinic. Computerworld, 40(7), 1.
46. Wechsler, J. (2007). Health IT implementation slows down. Managed Healthcare Executive, 17(7), 12.