A deeper look into today’s electronic health record

Health & Medicine, Healthcare

ASSIGN BUSTER

A Deeper Look into Today’s Electronic Health Record Alexandria Carroll Hodges University HIM 2501 Professor Shelye Mishler March 25, 2013 In the healthcare arena, information is everywhere and it is accessed and utilized by everyone. Information is the lifeblood of any organization and no organization would exist without it (Phillips, 2005). Regardless if the information is in paper form or accessed through a computer, there is a process needed to locate, retrieve, and evaluate the information. Since the onset of former President George W. Bush's steps to transform the health care delivery system through the adoption of interoperable electronic health records (EHR), the nation has shifted toward the use of EHR (Dunlop, 2007). The very basics consist of data which is an uninterrupted element. A collection of data is processed and then displayed as information. When data and information are brought together, knowledge results and decisions can be made. The electronic health record consists of any information as related to the patient's past, present or future conditions both mental and physical (Englebardt & Nelson, 2002) from birth to death. The key to EHRs and the vision to reduce patient errors while attaining optimal patient outcomes is interoperability. Interoperability enables the patient's information to become accessible and shared to providers and other healthcare systems when and where they need it. It is true to say that interoperability is fundamental to the success of EHRs (Heubusch, 2006). EHRs and the electronic world healthcare is entering will be creating an enormous amount of information that will necessitate organization and management. Health care produces vast amounts of information. This information must be collected, monitored, stored, retrieved and utilized to be beneficial to an organization. Quality of care is directly related to the quality of information available to healthcare professionals (Elliott & Watson, 2007) and managing such information is crucial. Systems would become fragmented and would no longer be beneficial if information lacks planning and organization. When we consider data, we think of it to be a fact about something or anything such as an object, thing or event. One piece of fact is considered one piece of data; therefore a collection of data that is structured is considered a database. In the healthcare arena, imagine all the pieces of data that are created and structured into a database. The healthcare industry is in a time of great change where the adoption of electronic healthcare records (EHR) are opening new opportunities for medical knowledge that will enhance the quality of care, reduce costs and promote services for physicians, nurses, administrators and consumers (Fickenscher, 2005). The adoption of EHRs will also inherit the vast amount of data that are generated through the health care process (Prather, Lobach, Goodwin, Hales, Hage & Hammond, 1997) whereas the data will be retrieved, accesses, evaluated and analyzed. This is made possible by a database management system (DBMS) which is a program that enables a user to manage, organize, store, and retrieve data and information from a database (Englebardt & Nelson, 2002). A database is the file cabinet that stores the data in a computerized hierarchy of field, record and file (Englebardt & Nelson, 2005). A critical issue to information technology and electronic health records is the privacy, confidentiality and security of all health information. The Health Insurance Portability and Accountability Act (HIPAA) of 1996 has forced hospitals to change polices regarding privacy and confidentiality (Homsted L., 2007). Security of health information is not only mandated by the hospitals but it is the law as authorized by the Department of Health and Human Services. To alleviate the issues, hospitals are responsible for utilizing technologies to safeguard inappropriate use for patient safety. Therefore, it is imperative to comply with hospital's policies and procedures regarding HIPAA. One cannot retrieve information other than as defined by their job; they cannot share passwords, look up information for others as well for self if it is not work related. Violations of practices can lead to termination. Patient information cannot be shared unless they sign an informed consent for treatment or payment purposes (Pearson, L., 2001). Respect for the patient is crucial and unless you need to know, the information should remain private, secure and confidential. Information technology is rapidly evolving among the health care systems that will provide information to improve the quality of patient care. Another critical issue to information technology and electronic health records is the privacy, confidentiality and security of all health information. It is important for all organizations to realize that confidentiality, and the issue of data acquisition, storage and release is a major topic in society today and not just a topic of conversation in the hospital sector (Fullbrook, 2007). Security of health information is not only mandated by the hospitals but it is the law as authorized by the Department of Health and Human Services. Information security should be the responsibility of the information system (IS) administration (Englebardt & Nelson, 2002). The Health Insurance Portability and Accountability Act (HIPAA) of 1996 increased the standards and have forced hospitals to change policies regarding privacy and confidentiality (Homsted, 2007). Data security involves protecting data from theft, malicious destruction and from unauthorized updating (Gillenson, 2005). Undesired access includes access policy violations, unauthorized access to systems or data and attacks that enable an individual or computer device to gain inappropriate access to information that should be restricted. The most well known threat includes e-mail viruses, spyware, and protocol abuse that will cause slow operation of desktop or lead to leakage of protected health information. Clark (2008) notes this year the healthcare industry had a few breaches with high profile celebrities whereas healthcare facilities are seriously re-evaluating the current situation of security and the healthcare industry. These situations represent the challenges hospitals face with access and authentication to patient data. Authentication is used to prove the identity of individuals accessing health data over a network which allows tracking and auditing validity (Englebardt & Nelson, 2002). The first line of defense to prevent unauthorized entry is the need for a password in combination of an identification tag. Identification tags are known within the company but the passwords are to be kept secret, not written down, accessible for others to witness and should be changed periodically (Gillenson, 2005). Passwords should be easy to remember, not too long or too short and they should not be obvious. One way to target these challenges is choosing to implement a single sign-on (SSO) solution to assist with HIPAA's security requirements. SSO would require an employee to use and remember one set of credentials to access the authorized applications. A single sign-on would strengthen password security, enforces net work authentication as well as tracking for audits and security. SSO enables facilities to implement an additional layer of security. At the data base management system level, the user would not be allowed to access any data wanted but would require specific privileges to specific data. In addition, only certain databases can be accessed as well as only certain data within the certain database. Furthermore, access to the data base can be restricted to read only user or an update, insert or delete user. The weakest part of data security infringement is the users. Computer usage in the healthcare environment has become a norm where various databases are being accessed and utilized. Sharing of passwords or carelessness with passwords enables other to access information that is not directly related to their scope of practice. Training employees on data security measures is an important strategic method to ensure security. Trained and knowledgeable employees as well as the software designers, developers, trainers and maintenance staff are essential for safe use. Security and privacy to patients, healthcare entities and providers will be a challenge as electronic health records, and the development of other new applications embrace all stakeholders in the healthcare domain. Although clinical information systems were identified as one of the most important applications for the next two years, financial support for IT continues to be a barrier. Former president George Bush, in 2004, mandated EHR to be established by 2010 due to the findings of Institute of Medicine releasing that EHR would facilitate patient safety (Bodin, 2007). Electronic health records can increase communication and promote interoperability among multiple medical facilities. My current facility encompasses four hospitals, hospital based physician offices, outpatient clinics, cancer center, rehabilitation center, and convenient care centers along with integration of facilities outside the network. EHR has the ability to make data immediately accessible to multiple entities at the same time (Simpson, 2001). The overall consensus of the research findings supported that EHR did indeed reduce errors and promoted patient safety with optimal outcomes. Kossman, & Scheidenhelm, S. L. (2008) found 25% to 98% of nurses’ work was utilizing EHR. The report also noted that nurses found EHR had the ability to “ speed up medication process, get reports and to communicate with other facilities". An ambulatory care service also noted benefits from EHR stating “ in the ambulatory care setting, IT helps support the immediacy of care and the caseload of patients" (Lofstrom, J. & Sensmeier, J., 2006). In addition, slow computers, downtime, and not enough computers hindered their work and impeded their time. Research found the ICU arena also benefited from implementing an EHR, whereas, large amounts of clinical data were captured and provided assistance to critical decision making with the ability to interface with medical devices from other facilities was a tremendous value (Zytkowski, M. E. & Abbott, P. A., 2003). Moreover, it is clear that electronic health records’ positives outweigh the negatives. In researching the various articles, the negatives I found were few. Nurses spending more time at computers either entering or retrieving information led to less time with the patient (Kossman & Scheidenhelm, 2008). In addition, computers that are slow, not having enough computers and down time could interfere with time and organization. What happens when “ new" staff members who have been trained in the technologic era of EHR are faced with a system that is “ down"? Will staff members be able to function as well and be able to continue with patient care? Would patient safety be compromised creating poor patient outcomes? It is a question I

have regarding the negative impact of EHR if informaticians are not ready with a plan in the computerized environment. Bodin, S. (2007). Evidence and nursing informatics to improve safety and outcomes. Nephrology Nursing Journal, 34(2), 135-136. Dunlop, L. (2007). Electronic health records: Interoperability challenges patients' right to privacy. Shidler Journal for Law, Commerce + Technology, 3(16), 1-15. Retrieved from http://www. lctjournal. washington. edu/vol3/a016dunlop. html. Englebardt, S. P. & Nelson, R. (2002). Healthcare Informatics: An Interdisciplinary Approach. St. Louis, MO: Mosby. Fullbrook, S. (2007). Confidentiality. Part 3: Caldicott guardians and the control of data. British Journal of Nursing, 16(16), 1008-1009. Heubusch, K. (2006). Interoperability: What it means, why it matters. Journal of American Health Information Management Association, 77(1), 26-30. Homsted, L. (2007). Confidentiality and privacy in the " Techno-world" of the internet. The Florida Nurse, 2-3. Kossman, S. P. & Scheidenhelm, S. L. (2008). Nurses’ perceptions of the impact of electronic health records on work and patient. CIN: Computers Informatics Nursing, 26(2), 69-77. doi: 10. 1097/01. NCN. 0000304775. 40531. 67 Lofstrom, J., & Sensmeier, J. (2006). Ambulatory informatics nurses: Translating the language of patient care. American Academy of Ambulatory Care Nursing, 28(5), 3-6, 11. Pearson, L. (2001). E-health and HIPAA: Important emerging issues affecting our practice. The Nurse Practitioner, 26(4), 12-14. Phillips, J. (2005). Knowledge is power: using nursing information management and leadership interventions to improve services to patients, clients and users. Journal of Nursing Management, 13(6), 524-536. Simpson, R. L. (2001). Mapping an IT career: the future of nursing. Nursing Administration Quarterly, 25(2), 80-85.

Zytkowski M. E. & Abbott, P. A. (2003). Nursing informatics: The key to unlocking contemporary nursing practice. Advanced Practice in Acute and Critical Care, 14(3), 272-281.