A about: there is no security policy to guarantee the safety of the electronic he...

Safety of Electric Health Records An electronic health records system consists of a longitudinal compilation of health information for and about people in electronic form, where only authorized users are allowed access to the system on both the person and population levels, and whose functions include provision of data and decision support for the improvement of the quality, safety and efficiency of health care delivery for patients (Carter, 2008). It is my position that since there is no unified policy to ensure the safety of electronic health records, there is always the possibility that information stored in electronic health records system might be compromised. The following exposition supports my stand on this issue. Walsh, Passerini, Varshney, and Fjermestad (2010) underscored a number of unresolved issues pertaining to the use of electronic health records (EHR), specifically along the areas of security and privacy. Walsh, et al. (2010) categorically stated that " electronic health records may not be secure" (p. 325). Their position stems from the fact that EHR systems are generally Web-based and could fall as easy prey to hackers who are adept at penetrating wireless networks or intercepting information while in transmission. Additionally, Bloebal (2002) identified a number of possible scenarios which could ensue when the safety of EHR systems are compromised and health professionals are misled, including administration of wrong treatment, withholding of the right to treatment, or delays due to lack of patient information. While the Health Insurance Portability and Accountability Act (HIPAA) established standards for the safety of health information, and mandates both efficiency and security in the EHR since 1996, there is failure on the part of HIPAA to adequately protect patient information on grounds that it permits entities (i. e. health plans providers,

health care professionals, health care clearing houses; business associates, etc) to do their own thing in protecting sensitive data. In this regard, HIPAA functions to serve public interest, but not personal interest in the privacy of health information (Carter, 2008). Confusingly, Walsh, Passerini, Varshney and Fjermestad (2010) reported that the US Department of Health and Human Services (HHS) issued the first set of standards for EHR in July last year to reinforce EHR security and reliability. If the HHS standards are the first, what then were the standards enforced by the HIPAA? In the same vein, there was confirmation regarding the existence of differing system standards in the usage of EHR, and that there were " no standards or only partial standards are in place" (Walsh, et al., 2010, para. 9). To date, it may be said that even if groundwork for the national implementation of EHR in the US had been laid since the administration of Pres. George W. Bush, the final rule on standards has yet to take effect. Meanwhile, health care entities which conform to different standards may not share data with one another (Walsh, et al., 2010). This suggests that records from one system may not be migrated to another system even if attempts for unification into one final set of standards are made – definitely not an indication of meaningful data use (American Recovery and Reinvestment Act, 2009). This eventuality does not only defeat the purpose of automating health records, but puts to waste the millions already doled out as incentives to reward entities which adopted and supposedly made meaningful use of their health records systems. If the use of electronics records will be enforced on the national level by 2014, an all-encompassing and unified policy on standards should be put in place not later than this year. Only in a unified no-nonsence policy will the safety of electronic records be appropriately safeguarded. References American

Recovery and Reinvestment Act (2009). Retrieved http://frwebgate. access. gpo. gov/cgi-bin/getdoc. cgi? dbname= 111_cong_bills&docid= f: h1enr. pdf Bloebal, B. (2002). Secure communication & co-operation of distributed electronic patient records. In F. Mennerat (Ed.), Electronic health records and communication for better health care: Proceedings of EuroRec ’01 (pp. 28-37). Amsterdam, NDL: IOS Press. Carter, J. H. (2008). Electronic health records: a guide for clinicians & administrators (2nd ed.). Philadelphia, PA: American College of Physicians. Halamka, J. D., Frisse, M. E., Dentzer, S. & Agres, T. (Eds.). Electronic health record standards. Retrieved from http://www. healthaffairs. org/healthpolicybriefs/ brief. php? brief_id= 26 Walsh, D., Passerini, K., Varshney, U. & Fjermestad, J. (2010). Legal issues in the transition to electronic records in health care. In A. D’Atri & D. Sacca (Eds.), Information systems: people, organizations, institutions & technologies (pp. 321-327). Heidelberg, DEU: Springer Verlag.