A systematic literature review of Security, Privacy and Confidentiality of patient information in Electronic Health Information Systems

D. B. A. Saranga Jayawardena MBBS, MSc (Medical Administration)
Regional Director of Health Services Office, Kalutara, Sri Lanka
E-mail address: jayawardenaayanthi@ymail.com

Sri Lanka Journal of Bio-Medical Informatics 2013;**4**(2):25-31
doi: http://dx.doi.org/10.4038/sljbmi.v4i2.5740

Abstract

Introduction
The evolution of medicine during the past few decades has resulted in electronic transformation of patient records which experienced multiple problems such as security, privacy and confidentiality of patient's information. Security, privacy and confidentiality are potentially major problems in electronic health records and no system currently available in the world is 100% secure. The objectives of this study were to describe the major issues related to security, privacy and confidentiality of electronic health information systems and computer based patient record systems and to describe methods currently used to overcome those issues by reviewing published articles.

Method
These articles were identified by searching the PubMed online electronic bibliographic database [www.ncbi.nih.gov/pubmed] for articles published between January 2000 and January 2013 using the keywords security, privacy, confidentiality, electronic health information systems, and computer based patient record systems. 25 articles were selected for this review after a screening process from among 236 articles identified after the PubMed search.

Results
All 25 articles (100%) had identified that security, privacy, and confidentiality were major problems with Electronic Health Records. None of them were 100% secure and only two (8%) were Health Insurance Portability and Accountability Act (HIPAA) compliant.

Conclusion
Safeguarding the security, privacy and confidentiality is a major problem in electronic health records and a major challenge for governments. However, studies on the security, privacy and confidentiality issues were not conclusive. Alternative approaches considering social, cultural and governmental factors may be needed to be taken into account to deal with the security, privacy and confidentiality issues.

Keywords - Privacy; Security; Confidentiality; Electronic Health Information Systems

Introduction

Electronic Health Records and digitalisation of patient records are emerging new trends in health services all over the world because digitising health information has helped to improve the quality of health care services. This has resulted in multifarious issues related to security, privacy and confidentiality of patient information[(1)]. The term *'privacy'* has been defined as an individual's desire to limit the disclosure of personal information. The term *confidentiality* refers to a process in which information should be released in a controlled manner. The term *security* refers to the measures that an organisation develops for protection of information[(1)]. Several Electronic Health Record Systems have been developed but all have functional weaknesses[(3)]. Security, privacy and

confidentiality are potentially major issues in electronic health records. There is no system in the world currently available which is 100% secure and uncrackable[2,3,4,5]. Medical administrators should pay attention to implementing proper control measures and at the same time installing electronic health information systems in a manner protecting the system from unauthorised access[3].

The objectives of this study were to describe the major issues related to security, privacy and confidentiality of electronic health information systems and computer based patient record systems and to describe methods currently used to overcome those issues by reviewing published articles.

Methods

These articles were identified by searching the PubMed online electronic bibliographic database [www.ncbi.nih.gov/pubmed] for articles published between January 2000 and January 2013 using the keywords security, privacy, confidentiality, electronic health information systems, and computer based patient record systems.

Results

A total of 236 articles were identified at the end of this process. After careful analysis of the 236 articles, 211 (89.41%) of them were excluded because in 7 (2.97%) the abstract was not available, in 43 (18.22%) the full text article was not available, in 115 (48.73%) the article did not deal with security, privacy or confidentiality issues, and in 46 (19.49%) the articles were published before the year 2000. The remaining 25 (10.59%) articles were used for this analysis.

All 25 articles (100%) had identified that security and confidentiality were major issues with electronic health records. None of them described 100% secure systems[4,5]. Electronic health information systems are potentially vulnerable to authorised or unauthorised access and to misuse of sensitive information. Authorised users may access information with their legitimate authority but with no valid reason for the access, often it may be due to personal interest regarding a relative or a friend or to divulge sensitive information to outsiders who cannot access such information.

They have more opportunities than outsiders to disclose sensitive information inappropriately. This is an unethical practice which is difficult to stop. Unauthorised attackers may access the systems to delete, misuse, destroy, change or steal sensitive data preventing authorised users legitimate access[1,5,6].

Concerns and solutions regarding data protection issues

Most of these articles[4-25] have discussed about security and privacy concerns and most of them[6-25] described the introduction of some solutions to safeguard the security of the records and to protect patients' privacy on health information.

One study was designed to highlight health service consumers' (i.e. Patients/Public) attitudes and concerns about the security and privacy issues of electronic health records (EHRs)[4]. Health service providers' (clinicians) view on data protection issues was discussed in one study[9]. The major privacy and security issues highlighted were unauthorised access to EHRs, unauthorised disclosure of sensitive data, potential misuse of these data for fraud and the alteration of data

without the owner's permission[4,6,9]. One study[4] reported that the majority of patients were very concerned about the privacy and security of their EHRs, but many believed that the benefits of EHRs outweigh privacy and security concerns. Thus majority wanted to limit access to their EHRs among non medical personal but not the physicians who were involved with their treatment[4,9].

Three articles[5,6,16] described effective ways of protecting electronic health information, data de-identification and anonymisation. But in this process there will be a re-identification risk for medical reports and there will be missing data and in some instances where alteration of data may occur. Two papers have discussed about re-identification attacks on health data associated with data de-identification methods[6,17]. One article introduced a privacy protection method with a solution for re-identification risk viz. Hiatus Tailor system where it identifies high risk data in the database for better information management with much lower information loss[6].

Two (8%) articles[7,8] described systems that were compliant with the Health Insurance Portability and Accountability Act (HIPAA). Both of them have assessed security and privacy characteristics according to the HIPAA standards. One[7] showed a number of differences in the analysed characteristics of Personal Health Records (PHR) and HIPAA standards while the other[8] highlighted that state law have more protective elements of confidentiality than that of HIPAA.

Some articles have discussed about access control managements to increase patient empowerment for their personal information protection[10,13,19]. A systematic literature review [10] had discussed about EHR systems that have access control management methods. It revealed that most of the systems with access control methods have consumer access control mechanisms as well as health professional access control mechanisms thus ensuring the patients' privacy right to control their personal information.

One article[13] described a system that had introduced a data protection technical solution based on web security standards. USA, Australia and many other countries have made provisions for expanded health information privacy protection in their constitutions and they have also amended legal coverage by introducing new acts that strengthen security and privacy standards in health information[20,21,22,23].

Two articles[15,20] have highlighted the need for transparency of data and the need for a national framework addressing access and control of secondary use of data[15]. Some articles[22,23,24] have identified that EHRs pose a greater risk of losing privacy in health data and authors state the importance of formulating a new policy on recording health data in order to protect privacy concerns.

Privacy and confidentiality concerns in special occasions in EHRs

Mental health information which contains highly sensitive information has to be specially considered when taking protecting privacy and security of databases, because if privacy is breached then patients' trust will be affected. There were instances where privacy of mental health databases have been breached[8,9].

One (4%) paper[25] discussed the protection and security of genetic/genomic test information and it highlighted that genetic/genomic test information should be treated differently from other medical data as they contain more personalised information and these information should be

protected to secure the trust of patients.

Summary

In all papers reviewed security, privacy and confidentiality concerns were highlighted and they had resulted in greater caution on acceptance of storing personal information in EHRs. Future developers of software for electronic health record databases should be very cautious about protecting health service consumers' privacy and confidentiality. The success of the implementing EHR systems will depend on the ability to protect security, privacy and confidentiality of information in these systems.

Conclusion

It is hoped that this review, based on 25 articles published between 2000 to 2013 would contributed to a better understanding of the relationship between security, privacy and confidentiality of patient information and electronic health records. Safeguarding the security, privacy and confidentiality is a major problem in electronic health records and a major challenge for governments. It is clear that these should be addressed in health policy development for electronic health information systems. There should be legal cover on patients' privacy protection, security of patients' health records and confidentiality of electronic health records. However, studies on the security, privacy and confidentiality issues are not conclusive. Alternative approaches, taking into account social, cultural and governmental factors, may have to be developed to deal with security, privacy and confidentiality issues.

References

1. Committee on Maintaining Privacy and Security in Health Care Applications of the National Information Infrastructure and Computer Science and Telecommunications Board Commission on Physical Science, Mathematics and Applications National Research Council, For the Record Protecting Electronic Health Information, National Academy Press, Washington, D.C. 1997. ISBN: 978-0-309-05697-7. Available at http://www.nap.edu/catalog/5595.html

2. Barrows R.C, Clayton P.D., Privacy, confidentiality: and electronic medical records. Journal of the American Medical Informatics Association 1996; **3**:139-48. http://dx.doi.org/10.1136/jamia.1996.96236282

3. Fisher F, Madge B, Data security and patient confidentiality: the manager's role, International Journal of Biomedical Computing 1996; **43**(1-2):115-9. doi: http://dx.doi.org/10.1016/S0020-7101(96)01236-6

4. Tejero A., De la Torre I. Advances and current state of the security and privacy in electronic health records: survey from a social perspective. Journal of Medical Systems 2012; **36**(5):3019-27. doi: http://dx.doi.org/10.1007/s10916-011-9779-x.

5. Virone M.G. EHR and data protection issues in Italy. Students Health Technology Information 2012; **180**: 741-5.

6. Li F, Zou X., Liu P, Chan J.Y. New threats to health data privacy. BMC Bioinformatics 2011; 12 Suppl 12:S7.
doi: http://dx.doi.org/10.1186/1471-2105-12-S12-S7

7. Ya L.C, Bo C.C, Hsueh L.C, Chia I.L, Guo T.L. et.al. A Privacy-preserved analytical method for eHealth database with minimized information loss. Journal of Biomedicine and Biotechnology 2012(2012); Article ID 521267, 9 pages.
doi http://dx.doi.org/10.1155/2012/521267

8. Carrion I, Aleman J. L, Toval A. Assessing the HIPAA standard in practice: PHR privacy policies. Annual International Conference Proceeding of Institute of Electrical and Electronics Engineers (IEEE) - Engineering in Medicine and Biology Society 2011; **2011**:2380-3.
doi: http://dx.doi.org/10.1109/IEMBS.2011.6090664

9. Clemens N.A., Privacy, consent and the electronic mental health record: The person vs the system. Journal of Psychiatric Practice 2012; **18**(1):46-50.
doi: http://dx.doi.org/10.1097/01.pra.0000410987.38723.47

10. Salomon R.M, Blackford J.U, Rosenbloom S.T, Seidel S, Clayton E.W. *et.al.* Openness of patients' reporting with use of electronic records: psychiatric clinicians' views. Journal of the American Medical Informatics Association 2010; **17**(1):54-60.
doi: http://dx.doi.org/10.1197/jamia.M3341

11. Carrion S.I, Ferdinandez A.J.L, Toval A. Access control management in electronic health records: a systematic literature review. Journal of Gaceta Sanitaria 2012; **26**(5):463-8.
doi: http://dx.doi.org/10.1016/j.geceta.2011.11.019.

12. Chen Y.Y, Lu J.C, Jan J.K. A secure EHR system based on hybrid clouds. Journal of Medical Systems 2012; **36**(5):3375-84.
doi: http://dx.doi.org/10.1007/s10916-012-9830-6

13. Das S, Kundu M.K, Effective management of medical information through a novel blind watermarking technique. Journal of Medical Systems 2012; **36**(5):3339-51.
doi: http://dx.doi.org/10.1007/s10916-012-9827-1

14. Falcao R.F, Costa P.A, Correia M.E. Access and privacy rights using web security standards to increase patient empowerment. Student Health Technological Information 2008; **137:**275-85.

15. Ray P, Wimalasiri J. The need for technical solution for maintaining the privacy of EHR Annual International Conference Proceeding in Institute of Electrical and Electronics Engineers (IEEE) - Engineering in Medicine and Biology Society.2006; **1**:4686-9.
doi: http://dx.doi.org/10.1109/IEMBS.2006.260862

16. Tejero A, de la Torre I, Advances and current state of the security and privacy in electronic health records: survey from a social perspective. Journal of Medical Systems 2012;

36(5):3019-27.
doi: http://dx.doi.org/10.1007/s10916-011-9779-x

17. Blobel B, Authorization and access control for electronic health record systems. International Journal of Medical Information 2004; **73**(3):251-7.
doi: http://dx.doi.org/10.1016/j.ijmedinf.2003.11.018

18. Coiera E, Clarke R. e-Concent: The Design and Implimentation of consumer concent mechanisms in an electronic environment. Journal of American Medical Information Association 2004; **11**(2):129-140.
doi: http://dx.doi.org/10.1197/jamia.M1480

19. Dimitropoulos L, Patel V, Scheffler S.A, Posnack S. Public attitudes toward health information exchange: Perceived benefits and concerns. American Journal of Management Care 2011; **17**(12 Spec No.):SP111-SP116

20. Safran C, Bloomrosen M, Hammond W. E, Labkoff S, Markel-Fox S. et.al. Toward a national framework for the secondary use of health data: An American medical informatics association white paper. Journal of American Medical Information Association 2007; **14**(1):1-9.
doi: http://dx.doi.org/10.1197/jamia.M2273

21. Beard L, Schein R, Morra D, Wilson K, Keelan J. The challenges in making electronic health records accessible to patients. Journal of American Medical Information Association 2012;**19**(1):116-120.
doi: http://dx.doi.org/10.1136/amiajnl-2011-000261

22. Goldstein M, The health privacy provisions in the American Recovery and reinvestment Act of 2009: Implications for Public Health Policy and Practice. Public Health Reports 2010; **125**(2):343-349.

23. Murphy S.N, Gainer V, Mendis M, Churchill S, Kohane I. Strategies for maintaining patient privacy in i2b2. Journal of American Medical Information Association 2011;18 (Suppl1): i103-i108.
doi: http://dx.doi.org/10.1136/amiajnl-2011-000316

24. Haas S, Wohlgemuth S, Echizen I, Sonehara N, Muller G. Aspects of privacy for electronic health records. International Journal of Medical Information 2011; **80**(2):e26-31.
doi: http://dx.doi.org/10.1016/j.ijmedinf.2010.10.001

25. Liu H.H. Use and disclosure of health information and protection of patient privacy in Taiwan. Medical Law 2010; **29**(1):87-101.

26. Peng C, Kesarinath G, Brinks T, Young J, Groves D. Assuring the privacy and security of transmitting sensitive electronic health information. AMIA Annual Symposium Proceedings Archive 2009;2009:516-520.

27. McGuire A.L, Fisher R, Cusenza P, Hudson K, Rothstein M.A..*et.al*. Confidentiality, privacy, and security of genetic and genomic test information in electronic health records: point to consider. Genetics in Medicine 2008; **10**(7):495-9.
doi: http://dx.doi.org/10.1097GIM.0b013e31817a8aaa.