Journal of Engineering and Applied Sciences 12 (Special Issue 10): 9006-9012, 2017
ISSN: 1816-949X

Security Methodologies for Electronic Health Record: A Case Study

Mahendra Vucha, Himaja Anubolu, A.L. Siridhara and R. Karthik
Department of Electronics and Communication Engineering,
MLR Institute of Technology, Dundigal, Hyderabad, India

Abstract: Although, many safeguards and security policies have been proposed for Electronic Health Record (EHR), the need of privacy and security for EHR systems persists. This study presents the literature review and features of frequently adopted security policies for EHR systems. In this study, the literature of security techniques and methods adopted for EHR systems have been collected until 2016 and then techniques were analyzed to identify best security method for maintaining nation health records. This survey highlights the features that are essential for security policies of EHR systems and it also presents the technical features and mandate access control methods through proper cryptography architectures for the nation health record and Health Information Exchange (HIE) among the nations.

Key words: Electronic health record, cryptography architecture, health information exchange, privacy, data security, EHR systems

INTRODUCTION

Nowadays, the study based patient health records are being converted into Electronic Health Records to provide effective and real time services to the patients with acceptable flexibility in Health Information Exchange (HIE). The EHR system enables the health providers to easy access and sharing of patient health information but literature states that patients are disinclined in sharing their health information with other than the directed health care providers. So, the EHR system demands protection and security to enable authentication to access and share patient health information. The sharing of EHR raises noticeable concerns with patient health privacy and security. Privacy brings right to the patients about handling of their personal information disclosure where as data security provides protection to patients personal information against accidental, unlawful destruction and unauthorized access and disclosure. The privacy and security assures the EHR system and provide quality health services to the patients. The health providers have adopted some methodologies and standards in order to enhance the security to EHR. The worldwide adopted standards in various developed countries: USA-Health Level Seven (HL7), Health Information Technology for Economic and Clinical Health Act (HITECH) and Health Insurance Portability and Accountability Act (HIPAA), CANADA-Canada Health Infoway, JAPAN-HEASNET and EUROPE-ISO/TC 215, CEN/TC, etc.

As the privacy and security has become an important aspect for maintaining and sharing patient health information, the survey is limited to the technical plans which lead to the findings of technical solutions. Fernandez-Aleman *et al*. (2013) presented a security and privacy standard ISO 27799 to address security of EHR in terms of confidentiality, integrity and availability of patient health data. These security ISO standards can be implemented for many more real life applications such as compliance, acquisition, access control, communication and security policy, physical and environmental security. The ISO 27799 demonstrates information security and management schemes for EHR rather than the general technical schemes. This survey describes the security standards such as ISO/IEC 29100: 2011 and ISO/IEC 27002: 2013 which demonstrate security and privacy guidelines.

The ISO/IEC 27002: 2013 demonstrates information security and management practices for organisation information security risk environment. This ISO 2013 standard described 14 information security and control policies for organisation, human resources, asset management, physical and environment, communication, system acquisition and supplier relationships.

The ISO/IEC 29100: 2011 demonstrated cryptography framework for protection of personally identifiable information in EHR systems and also support security of information technology. The ISO 2011 standard describes 11 privacy policies for information security.

Literature survey on security attributes and standards: This study provides state of art of various security attributes, policies, standards and architectures adopted for securing patient health information in EHR.

Corresponding Author: Mahendra Vucha, Department of Electronics and Communication Engineering,
MLR Institute of Technology, Dundigal, Hyderabad, India

Access control standards: Access control strategies and policies are significant in ensuring security for EHR systems. The access control is very important aspect in providing confidentiality to EHR but it limit the access rights of patient data to the system users. The broker based access control is one of the access control mechanisms adopted for bringing confidentiality to information records. The access control employ privacy policies in providing access to only authorized health parties when health information database contain patient's personal identification information (Bouhaddou *et al*., 2012; Chen *et al*., 2012; Murray *et al*., 2011; Wu *et al*., 2012; Bloble and Pharow, 2007). In literature, there is role based, attribute based and cryptographic access control (Bouhaddou *et al*., 2012; Martinez *et al*., 2013; Zhang *et al*., 2011) policies to provide flexibility and control the access of health information with respect to time (Singh *et al*., 2013). The attribute based access control is widely used in EHR systems as compared to role based because of flexibility in policy descriptions (Hsieh and Chen, 2012). XACML is an open access control policy language (Acharya *et al*., 2013) that has been used in many researches to define and demonstrate access control polices.

Secure communication standards: In order to exchange EHR data among multiple health care providers, a secure communication channel needs to be established using secure firewall mechanisms (Liu *et al*., 2012; Mackenzie *et al*., 2011; Tsai, 2010; Haak *et al*., 2003; Aljarullah and Masri, 2012) such as VPN (Blobel, 2000; Li *et al*., 2011; Bakers and Masys, 1999), network segregation and SSL/TLS (Blobel and France, 2001; Guo *et al*., 2012; Safran and Goldberg, 2000; Stingl and Slamanig, 2011; Khan and Sakamura, 2012; Afzal *et al*., 2011). The eTRON architecture demonstrated by Barber (1998) uses an authentication and hybrid access control schemes for secure communication. Therefore, encryption of communication channel instead of data encryption has become essential for secure EHR exchange. The encryption of communication standards addresses the policies for authentication, integrity, confidentiality, non-repudiation and accountability of EHR. In literature (Bouhaddou *et al*., 2012; Murray *et al*., 2011; Mackenzie *et al*., 2011; Blobel and France, 2001; Guo *et al*., 2012; Santos *et al*., 2011; Bloble and Pharow, 2007; Coleman, 2013), many researchers addressed methods such as HL7, EDIFACT, xDT and XACML for secure communication channels. The HL7 proposed standards and methodologies for secure health information exchange and retrieval through Secure Message Delivery (SMD) methods. These methodologies are prominent secure health messaging standards used in many countries like USA, Canada and Germany.

Secure compliance standards: Implementation of EHR systems must obey the security standards of HIPAA, HL7, access control and ISO EHR standards. The healthcare providers obey the vocabularies (Bouhaddou *et al*., 2012) and common standards to enable and enhance data exchange efficiently of EHR (Afzal *et al*., 2011; Santos *et al*., 2011). The literature on this research demonstrated the compliance of HIPAA and HL7 standards and also importance of common database platforms. HIPAA gives policy guidelines to establish privacy and security to health information systems (Liu *et al*., 2012). HL7 describes architecture for secure cryptography framework for secure health information exchange (Hsieh and Chen, 2012).

Interoperability standards: Interoperability is an attribute of security system that permits and coordinates information database systems in exchanging information among multiple resources in order to quick sharing of available information. The interoperability can bear few information security policies such as constraint of unauthorised access and disclosure on health data to maintain confidentiality, integrity and availability. In order to achieve the objective of Health Information Exchange (HIE) systems, the interoperability integrate different EHR data repositories. In literature, there are many articles addressed various methods of interoperability. The interoperability methods and policies are stated in CEN prENV 1306 interoperability (Laszewski *et al*., 2011). The Data Segmentation for Privacy (DS4P), Win and Fulcher (2007) proposed and aims to ensure interoperability standards to access patients health data across different EHR systems. An architecture has been proposed for HIE (Santos *et al*., 2011) by using HL7 V3 standard and that architecture brings significant security through interoperability. An interoperability model called eMOLST has been proposed to integrate health record systems among Healthcare Enterprises. Moreover, maintenance of continuous care documents can strengthen the policies for interoperability and portability (Acharya *et al*., 2013) of EHR. Initially, Broker based composite EHR authorisation brings interoperability to EHR by developing a small database system initially and then the concept is extended to organize the patient data in the local and public databases (Blobel, 2000). By Bakers and Masys (1999), the interoperable EHR have been presented using encapsulated and modularised applications. The methodologies in literatures can transform to design

service oriented architecture for satisfying the security requirements. The project bIT4, Laszewski *et al.* (2011) presented a telematics architecture for providing interoperability through independent computational methods.

Consent policy standards: The concepts of sharing and controlling patient's health information with EHR information centres and national clinical research networks, provide effective health care to the patients. Canada health centres recommended DAC and RBAC as privacy and secure access control mechanisms for patient consent (Barber, 1998). Few researches in literature states that the hospitals and healthcare providers are primarily responsible for intimating patients and obtain consent from them to disclose and share their health data to healthcare provide centres. A consent model is presented by Win (2005) and it states that, written patient consent is very important in creation of agreements and policies for patient health information exchange. However, the data privacy legislations and health record privacy Acts in developed countries like UK, NSW and healthcare professional's states that the healthcare provider can access patient data without patients consent in medical emergencies (Sun *et al.*, 2011; Blobel, 2004; Matteucci *et al.*, 2011). The literature also states that the healthcare provider should not force the patients to obtain their consent and use or disclose such patient health data for payments, treatments and healthcare operations (Murray *et al.*, 2011). The digital rights management techniques already have taken the steps to help and provide patient consent to EHR systems (Huang *et al.*, 2012). The ISO standards ISO/DTS 17975 and ISO/TS 27790:2009 demonstrated patient consent policies as privacy methods and profiles. The popular privacy methods for patient consent include Patient Identification Cross-Referencing (PIX) and Cross-Enterprise User Assertion (XUA). The Data Segmentation for Privacy (DS4P) demonstrated privacy policies for sharing and enabling patient health information database systems to achieve the objectives of privacy protection schemes (Win and Fulcher, 2007).

Privacy policies and regulation standards: The policy is the legal frameworks about rules and regulations, organizational and administrative rights and agreements to provide technical solutions in order to process and communicate information through recorded database systems (Huang *et al.*, 2012). In literature, there were privacy and security policies demonstrated for access control, authorisation, delegation, governing regulation, disclosure, sharing and integrating and medical regulations. Effective and information specific policies and procedures would help in achieving strong security and high level privacy for electronic records (Singh *et al.*, 2013; Safran and Goldberg, 2000; Toh *et al.*, 2011). Adopting common information sharing policies and regulations would help healthcare centres in providing specific solutions patient health information (Bouhaddou *et al.*, 2012; Santos *et al.*, 2011; Li *et al.*, 2013; Blobel and Pharow, 2006).

Flexibility standards: The role based and time bound access control provides privacy and flexibility for EHRs (Win, 2005) but the Attribute Based Access Control (ABAC) is effective as compared with role based access control adopted. Since, the ABAC brings flexibility and granularity to the EHR systems, suitable network architecture need to be established across different EHR to bring optimum scalability and security features for EHR systems (Blobel and Pharow, 2006). The scalability is necessary for distributed EHR systems in order to handle with big data (Blobel, 2000; Bakers and Masys, 1999). The flexibility play significant role in designing security for EHR with automatic decision making features during medical emergency (Bakers and Masys, 1999; Burton *et al.*, 2013). The flexibility and security of EHR systems offers interoperability to the systems while exchanging health information (Rodrigues *et al.*, 2013).

Applicability and scalability standards: Applicability and scalability enable the patient to access their health data from EHR even at outside home. The applicability and scalability standards also support patient and healthcare providers to access data instantly in medical emergency. The aim of scalability in EHR is to exchange patient health information through private and public network domain in order to support patient medical emergency (Singh *et al.*, 2013; Hsieh and Chen, 2012). Applicability of privacy policies to EHR systems is crucial in disclosure of patient health information (Wijayanti, 2017). The scalability supports in merging EHR systems into complex database systems (Burton *et al.*, 2013) called cloud computing environment.

Integration and sharing standards: The advancement in secure information sharing through cloud computing environment can provide security for Personal Health Record (PHR) and also it raises significant barriers to the EHR while storage, usage and access management of data (Chen *et al.*, 2012; Bloble and Pharow, 2007; Hsieh and Chen, 2012; Acharya *et al.*, 2013; Afzal *et al.*, 2011; Baldas *et al.*, 2010). There is need of defining standards for authenticity and integration of health information with

unsafe EHR systems in cloud. Matteucci *et al*. (2011) proposed a data sharing standards for sharing EHR data in controlled environment to assure confidentiality and data integrity. The sharing and integrating standards of HIE can integrate different nations to process health information through common interface and enable health care centres to provide quality health services (Santos *et al*., 2011). Adapting nation health information integrating standards for EHR system through centralised approaches can enhance the quality of services and also it controls the costs (Hsiao *et al*., 2012).

MATERIALS AND METHODS

Cryptography standards for EHR: This study demonstrates the methodologies adopted worldwide for maintaining and sharing of health records through secure channels.

Cryptography methodologies for health information records: Cryptography provides authentication, confidentiality, integrity and authorisation to the patient health information. These cryptographic security methodologies are classified into server security, user security and transmission security. The digital signatures based standards provides privacy to patient information through Trusted Third Party (TTP) and it helps in investigating non trusted medical information transactions and avoid illegal unauthorised services. Certificate Authority (CA) cryptography techniques has been presented (Neubauer and Heurix, 2011) as a TTP technique to issue security certificates and offers public supported services. The techniques like End-to-End Encryption (E2EE) for record authorisation and authentication may satisfy security requirements and also describe policies for access control (Hsieh and Chen, 2012). Pseudonymization of Information for Privacy in E-health (PIPE) framework has been presented by Riedl and Grascher (2010) to provide privacy and confidentiality for patient health record maintenance systems (Riedl and Grascher, 2010). The key in cryptography manages management crucial aspects such as storing, updating and revoking considered in cryptography (Burton *et al*., 2013). The public key encryption standards with keyword search security schemes provides patient controlled encryption, especially in fine-grained integrated systems (Acharya *et al*., 2013).

Cryptographic techniques for EHR business continuity: The business continuity of EHR demands integrity and availability of EHR systems. The EHR systems should available instantly for patient and healthcare providers in order to bring effective health services. The security control policies also required for communication channels to cooperate EHR systems and prevent any disruptions or failures (Chen *et al*., 2012; Aljarullah and Masri, 2012). The patient data in EHR need to be secured with technologies like digital clustering, RAID systems and back-up procedures in order to bring business continuity to the patients EHR in cloud server (Chen *et al*., 2012; Singh *et al*., 2013; Aljarullah and Masri, 2012; Blobel, 2000; Khan and Sakamura, 2012; Matteucci *et al*., 2011). So, the business continuity of EHR can be achieved by implementing cryptography techniques that bring high level of security and availability for EHR information in cloud computing designs (Chen *et al*., 2012; Hsieh and Chen, 2012; Acharya *et al*., 2013; Blobel, 2000; Khan and Sakamura, 2012; Li *et al*., 2013).

Accuracy and quality standards for EHR: The quality and accuracy standards provide services like security and privacy protection to the EHR systems. Integration of patient's health information with EHRs in cloud servers provides accuracy and consistency for data (Chen *et al*., 2012; Singh *et al*., 2013; Blobel and France, 2001; Li *et al*., 2013, 2011). The Patient Centred Access to Secure Systems Online (PCASSO) project improves the quality of health care and provides considerable privacy to patient health information by adopting right security methods like RBAC, multi level security and privacy authentication audit trails (Blobel and France, 2001). The appropriate quality assurance methods and health plans can provide confidentiality and security for EHR transactions through cloud servers.

Operations security for EHR: Operations security brings features like monitoring, auditing, archiving and restoring of patient health information in EHR systems. Auditing the records refers to maintenance of log in register for users and activities. Archiving means storing information in offline and restore them whenever required (Chen *et al*., 2012; Singh *et al*., 2013). Monitoring is very significant in transmitting data through secure communication channels and also in identification of suspicious activity to protect the data from malicious events. The EHR system needs to be adopted back-up mechanisms in order to ensure privacy to the patient health data for authorised users (Khan and Sakamura, 2012).

RESULTS AND DISCUSSION

This study presents finding of literature survey and their significance in secure health record

maintenance. The access control and privacy policies should be defined to EHR through cryptography ISO standards in order to provide significant security for patient health information. There are researchers in literature proposed many procedures and standards to provide efficient encryption and key management scheme. The cryptography control standards and policies play significant role in achieving information security goals such as confidentiality, integrity, authenticity and authentication. The literature survey demonstrates that the EHR systems demand secure communication for sharing health information. Encryption of communication channel addresses the proper data exchange standards and regulations and there were standards addressed in HL7, HITECH, HEASNET to ensure secure health data exchange in healthcare providers and clinical database systems. The data exchange networks need to be managed and controlled by defining cryptography implementations that provide security and protect patient health information from unauthorised access.

This survey demonstrates the research gap in secure exchanging of health information systems. Interoperability can address information security, information access and information retrieval of EHR systems when they adhere to acceptable formats and regulations. The principles like understandable, affordable and accessible mechanisms bring patient consent to health care providers in accessing health information at the right time at right place. This survey reveals the research gap on patient consent methods to define policies and standards that need to be considered while accessing information from EHR. Patient's can share the control and access rights of information to the authorised patients and healthcare providers and also to clinical research agencies. Patient consent states the ways of informing the patient and user about the processing of patients personal information. The healthcare providers should inform the patients about consent methods before processing their information and also need to inform the healthcare providers about the access rights of patient consent schemes.

Literature proposed few privacy policies and secure cryptographic architectures for flexibility of EHR systems. This survey uncovers the research gaps concerning to the flexibility policies of EHR systems. The proposed flexibility policies play major role in defining strategies for security of distributed EHR systems. An applicability and scalability policy of cryptography techniques ensures security of EHR systems. The survey suggests that there is need to emphasise security and privacy protection when sharing information of EHR systems. So, there is demand for defining agreements for security requirement in order to share information and provide coordination among security implementation techniques. The healthcare providers should adopt the proposed policies to share or integrate different EHRs. The literature on attribute strategies of EHR systems suggested right encryption schemes and access control policies to maintain EHR.

The literature survey demonstrated various security policies, controls access policies against malwares, technical exposure management standards, documented functioning procedures, policies on functioning software and their future updates. The survey described business continuity in health care should include utility and availability methods along with appropriate security protections for secure EHR systems. The business continuity ensures establishment of procedures and access controls policies for protecting available EHR system. So, healthcare providers can adopt redundancy requirements to meet the availability of EHR systems. The literature addressed quality and accuracy policies for maintaining EHR systems in order to provide quality services, healthcare and patient privacy. The study suggests operational accountability of networks, safeguarding policies of integrity, authentication policies for secure communication of EHR information. The information security policies presented review of technical standards for processing EHR information through secure cloud systems and servers. The growing complexity of ICT systems demand robust and secure processing standards to provide secure sharing and exchanging environment for patient health information.

CONCLUSION

The survey has been conducted to present secure and privacy standards for EHR systems. The survey demonstrated access control standards which are critical in providing privacy to patient health information while controlling the access rights of patient and healthcare providers with pre-defined access control policies and standards. Applicability of security and privacy standards to maintain EHR system demands cryptography specific frameworks. The EHR systems should comply with security requirements and standards to analyse and monitor the information security. The sharing and integration standards of EHR addressed increasing demands to patient's consent with standardized policies and access control strategies to authenticate patients healthcare systems in order to share health records through clinical networks. The interoperability standards make possible the health information access, exchange and retrieval through acceptable formats, standards and regulations. Availability standards provide security

operations including redundancy, organization of networking, network functioning responsibility, integrity and privacy, logging and authentication policies for secure communications. Accuracy, quality and flexibility policies must ensure enhanced healthcare system services.

REFERENCES

Acharya, S., B. Coats, A. Saluja and D. Fuller, 2013. Secure electronic health record exchange: Achieving the meaningful use objectives. Proceedings of the 46th IEEE Hawaii International Conference on System Sciences (HICSS), Januray 7-10, 2013, IEEE, Wailea-Makena,Hawaii,ISBN:978-1-4673-5933-7,pp: 2555-2564.

Afzal, M., M. Hussain, M. Ahmad and Z. Anwar, 2011. Trusted framework for health information exchange. Proceedings of the IEEE Conference on Frontiers of Information Technology (FIT), December 19-21, 2011, IEEE, Islamabad, Pakistan, ISBN:978-1-4673-0209-8, pp: 308-313.

Aljarullah, A. and S.E. Masri, 2012. A novel system architecture for the national integration of electronic health records: A semi-centralized approach. J. Med. Syst., 37: 9953-9953.

Bakers, D.B. and D.R. Masys, 1999. PCASSO: A design for secure communication of personal health information via the internet. Intl. J. Med. Inf., 54: 97-104.

Baldas, V., K. Giokas and D. Koutsouris, 2010. Multilevel access control in hospital information systems. Proceedings of the 12th Mediterranean Conference on Medical and Biological Engineering and Computing, May 27-30, 2010, Springer, Berlin, Germany, pp: 909-912.

Barber, B., 1998. Patient data and security: An overview. Intl. J. Med. Inf., 49: 19-30.

Blobel, B. and F.R. France, 2001. A systematic approach for analysis and design of secure health information systems. Intl. J. Med. Inf., 62: 51-78.

Blobel, B. and P. Pharow, 2006. Formal policies for flexible EHR security. Stud. Health Technol. Inf., 121: 307-316.

Blobel, B. and P. Pharow, 2007. A model driven approach for the German health telematics architectural framework and security infrastructure. Intl. J. Med. Inf., 76: 169-175.

Blobel, B., 2000. Advanced tool kits for EPR security. Intl. J. Med. Inf., 60: 169-175.

Blobel, B., 2004. Authorization and access control for electronic health record systems. Intl. J. Med. Inf., 73: 251-257.

Bouhaddou, O., T. Cromwell, M. Davis, S. Maulden and N. Hsing *et al*., 2012. Translating standards into practice: Experience and lessons learned at the department of veterans affairs. J. Biomed. Inf., 45: 813-823.

Burton, B., C. Cothran, N. Davis, J. Dooling and R. Dunn *et al*., 2013. The privacy and security of occupational health records. J. Am. Health Inf. Manage. Assoc., 84: 52-56.

Chen, Y.Y., J.C. Lu and J.K. Jan, 2012. A secure EHR system based on hybrid clouds. J. Med. Syst., 36: 3375-3384.

Coleman J., 2013. Segmenting data privacy: Cross-industry initiative aims to piece out privacy within the health record. J. Am. Health Inf. Manage. Assoc., 84: 34-38.

Fernandez-Aleman, J.L., I.C. Senor, P.A.O. Lozoya and A. Toval, 2013. Security and privacy in electronic health records: A systematic literature review. J. Biomed. Inf., 46: 541-562.

Guo, L., X. Liu, Y. Fang and X. Li, 2012. User-centric private matching for eHealth networks: A social perspective. Proceedings of the IEEE Symposium on Communication and Information System Security (GLOBECOM), December 3-7, 2012, IEEE, Anaheim, California, ISBN:978-1-4673-0920-2, pp: 732-737.

Haak, M.V.D., A.C. Wolff, R. Brandner, P. Drings and M. Wannenmacher *et al*., 2003. Data security and protection in cross-institutional electronic patient records. Intl. J. Med. Inf., 70: 117-130.

Hsiao, T.C., Z.Y. Wu, Y.F. Chung, T.S. Chen and G.B. Horng, 2012. A secure integrated medical information system. J. Med. Syst., 36: 3103-3113.

Hsieh, G. and R.J. Chen, 2012. Design for a secure interoperable cloud-based personal health record service. Proceedings of the IEEE 4th International Conference on Cloud Computing Technology and Science (CloudCom), December 3-6, 2012, IEEE, Taipei, Taiwan, ISBN:978-1-4673-4511-8, pp: 472-479.

Huang, C., H. Lee and D.H. Lee, 2012. A privacy-strengthened scheme for E-healthcare monitoring systems. J. Med. Syst., 36: 2959-2971.

Khan, M.F.F. and K. Sakamura, 2012. Security in healthcare informatics: Design and implementation of a robust authentication and a hybrid access control mechanism. Proceedings of the IEEE Mosharaka International Conference on Communications, Computers and Applications (MIC-CCA), October 12-14, 2012, IEEE, Istanbul, Turkey, ISBN:978-1-4673-5230-7, pp: 159-164.

Laszewski, G.V., J. Dayal and L. Wang, 2011. EMOLST: A documentation flow for distributed health informatics. Concurrency Comput. Pract. Experience, 23: 1857-1867.

Li, J.S., T.S. Zhou, J. Chu, K. Araki and H. Yoshihara, 2011. Design and development of an international clinical data exchange system: The international layer function of the Dolphin project. J. Am. Med. Inf. Assoc., 18: 683-689.

Li, M., S. Yu, Y. Zheng, K. Ren and W. Lou, 2013. Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption. IEEE Trans. Parallel Distrib. Syst., 24: 131-143.

Liu, C.H., Y.F. Chung, T.S. Chen and S.D. Wang, 2012. The enhancement of security in healthcare information systems. J. Med. Syst., 36: 1673-1688.

Mackenzie, I.S., B.J. Mantay, P.G. McDonnell, L. Wei and T.M. Macdonald, 2011. Managing security and privacy concerns over data storage in healthcare research. Pharmacoepidemiology Drug Saf., 20: 885-893.

Martinez, S., D. Sanchez and A. Valls, 2013. A semantic framework to protect the privacy of electronic health records with non-numerical attributes. J. Biomed. Inf., 46: 294-303.

Matteucci, I., P. Mori, M. Petrocchi and L. Wiegand, 2011. Controlled data sharing in E-health. Proceedings of the 1st Workshop on Socio-Technical Aspects in Security and Trust (STAST), September 8-8, 2011, IEEE, Milan, Italy, ISBN:978-1-4577-1182-4, pp: 17-23.

Murray, T.L., M. Calhoun and N.C. Philipsen, 2011. Privacy, confidentiality, HIPAA and HITECH: Implications for the health care practitioner. J. Nurse Pract., 7: 747-752.

Neubauer, T. and J. Heurix, 2011. A methodology for the pseudonymization of medical data. Intl. J. Med. Inf., 80: 190-204.

Riedl, B. and V. Grascher, 2010. Assuring integrity and confidentiality for pseudonymized health data. Proceedings of the IEEE International Conference on Electrical Engineering Electronics Computer Telecommunications and Information Technology (ECTI-CON), May 19-21, 2010, IEEE, Chiang Mai, Thailand, ISBN:978-1-4244-5606-2, pp: 473-477.

Rodrigues, J.J.P.C., I.D.L. Torre, G. Fernandez and M.L. Coronado, 2013. Analysis of the security and privacy requirements of cloud-based electronic health records systems. J. Med. Internet Res., 15: e186-e186.

Safran, C. and H. Goldberg, 2000. Electronic patient records and the impact of the Internet. Intl. J. Med. Inf., 60: 77-83.

Santos, C., T. Pedrosa, C. Costa and J.L. Oliveira, 2011. On the use of open EHR in a portable PHR. Proceedings of the 4th International Conference on Health Informatics (HEALTHINF), January 26-29, 2011, INSTICC Publisher, Rome, Italy, pp: 351-356.

Singh, R., V. Gupta and K. Mohan, 2013. Dynamic federation in identity management for securing and sharing personal health records in a patient centric model in cloud. Intl. J. Eng. Technol., 5: 2201-2209.

Stingl, C. and D. Slamanig, 2011. Health records and the cloud computing paradigm from a privacy perspective. J. Healthcare Eng., 2: 487-508.

Sun, J., X. Zhu, C. Zhang and Y. Fang, 2011. HCPP: Cryptography based secure EHR system for patient privacy and emergency healthcare. Proceedings of the 31st IEEE International Conference on Distributed Computing Systems (ICDCS), June 20-24, 2011, IEEE, Minneapolis,Minnesota,ISBN:978-1-61284-384-1,pp: 373-382.

Toh, S., R. Platt, J.F. Steiner and J.S. Brown, 2011. Comparative-effectiveness research in distributed health data networks. Clin. Pharmacol. Ther., 90: 883-887.

Tsai, F.S., 2010. Security issues in E-healthcare. J. Med. Biol. Eng., 30: 209-214.

Wijayanti, T.P., 2017. Knowledge management system design of Indonesian general district hospital. J. Eng. Appl. Sci., 12: 808-813.

Win, K.T. and J. Fulcher, 2007. Consent mechanisms for electronic health record systems: A simple yet unresolved issue. J. Med. Syst., 31: 91-96.

Win, K.T., 2005. A review of security of electronic health record systems. Health Inf. Manage. J., 34: 13-18.

Wu, R., G.J. Ahn and H. Hu, 2012. Secure sharing of electronic health records in clouds. Proceedings of the 8th IEEE International Conference on Collaborative Computing: Networking, Applications and Worksharing (Collaborate Com), October 14-17, 2012, IEEE, Pittsburgh, Pennsylvania, ISBN:978-1-4673-2740-4, pp: 711-718.

Zhang, R., J. Liu, Z. Han and L. Liu, 2011. RBTBAC: Secure access and management of EHR data. Proceedings of the IEEE International Conference on Information Society (I-Society), June 27-29, 2011, London, England, ISBN:978-1-61284-148-9, pp: 494-499.