A systematic literature review on security and privacy of electronic health record systems: technical perspectives

Fatemeh Rezaeibagha, Khin Than Win and Willy Susilo

Abstract

Background: Even though many safeguards and policies for electronic health record (EHR) security have been implemented, barriers to the privacy and security protection of EHR systems persist. **Objective**: This article presents the results of a systematic literature review regarding frequently adopted security and privacy technical features of EHR systems. **Method**: Our inclusion criteria were full articles that dealt with the security and privacy of technical implementations of EHR systems published in English in peer-reviewed journals and conference proceedings between 1998 and 2013; 55 selected studies were reviewed in detail. We analysed the review results using two International Organization for Standardization (ISO) standards (29100 and 27002) in order to consolidate the study findings. **Results**: Using this process, we identified 13 features that are essential to security and privacy in EHRs. These included system and application access control, compliance with security requirements, interoperability, integration and sharing, consent and choice mechanism, policies and regulation, applicability and scalability and cryptography techniques. **Conclusion**: This review highlights the importance of technical features, including mandated access control policies and consent mechanisms, to provide patients' consent, scalability through proper architecture and frameworks, and interoperability of health information systems, to EHR security and privacy requirements.

Keywords (MeSH): Electronic Health Records; Privacy: Data Security; Review, Systematic; Standards

Introduction

Currently, paper-based health record systems are moving toward electronic formats because electronic health record (EHR) systems provide efficient and real-time services to patients and create improvements in quality, flexibility and patient safety. Due to the digital nature of electronic healthcare systems, they are easily accessible and can be shared (Huang, Sharaf & Huang 2013). The crucial content of structured or free-text data contained in EHR systems determines that privacy and security protection are essential requirements to their management. Studies have also indicated that patients are reluctant to share their health information other than for direct clinical care (Li et al. 2011).

EHRs are shared among different systems and this openness raises considerable concern about patient privacy owing to the possibility of unauthorised access or misuse owing to improper security implementation (Zhang et al. 2011). Privacy means that patients have the right to handle the disclosure of their personal information (Lee, Chang & Wang 2013). Data security means the protection of personal information against 'accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access' (van der Haak et al. 2003). Due to the importance of patient data, it must be protected against malicious activities (Neubauer & Heurix 2011). In order to assure the security and privacy of EHRs while providing shared and interoperable EHR services, healthcare organisations have highlighted the importance of standards (Bouhaddou et al. 2012; Flores Zuniga, Win & Susilo 2010). Examples of such standard developers and publishers include: Health Level Seven (HL7), Health Insurance Portability and Accountability Act (HIPAA) and Health Information Technology for Economic and Clinical Health Act (HITECH) in the USA; Canada Health Infoway in Canada; HEASNET in Japan; and ISO/TC 215, CEN/TC in Europe (Khan & Sakamura, 2012).

As the security of EHR systems has been an important aspect in designing, implementing and managing the shared care paradigm, the requirements for such security and privacy of EHRs need to be identified to be applicable in such systems. To do this, we limited the search to the technical plans leading to limit the applicability of the findings to technical solutions. Then, we defined the following research question: 'What are the crucial security and privacy features of EHR systems from the technical perspective?' Fernández-Alemán et al. (2013) presented a security and privacy template based on ISO 27799,

which addresses health information security to ensure the level of security that is appropriate to an organisation's demands in order to maintain the confidentiality, integrity and availability of personal health information. This ISO standard has been categorised into the following: compliance; information systems acquisition, development and maintenance; access control; communication and operations management; information security policy; organising information security; asset management; physical and environmental security; information security incident management and human resources security (ISO 2008). The ISO 27799 focuses more specifically on the information security management perspective for EHR security than the technical perspective. In our study, we selected ISO/IEC 27002: 2013 (ISO 2013) and ISO/IEC 29100: 2011 (ISO 2011) standards, which focus more on security and privacy guidelines in light of a technical perspective.

The ISO/IEC 27002: 2013 gives guidelines for information security standards and management practices considering the organisation's information security risk environment and these cover information technology, security techniques, and information security management systems. This ISO standard contains 14 security control clauses: information security policies; organisation of information security; human resource security; asset management; access control; cryptography; physical and environmental security; operation security; communication security; system acquisition, development and maintenance; supplier relationships; information security incident management; the information security aspects of business continuity management and compliance (ISO 2013).

The ISO/IEC 29100: 2011 provides a framework for the protection of 'personally identifiable information (PII)' within information and communication technology (ICT) systems, which covers information technology, security techniques, and privacy. This ISO standard contains 11 privacy principles: consent and choice; purpose legitimacy and specification; collection limitation; data minimisation; use, retention and disclosure limitations; accuracy and quality; openness, transparency and notice; individual participation and access; accountability; information security and privacy compliance (ISO 2011).

In the following sections, we report a systematic literature review carried out according to the method advocated by Kitchenham et al. (2009), which has been followed by other researchers (Botella, Alarcon & Penalver 2013; De Oliveira & Soares 2012; Dos Santos, Delamaro & Nunes 2013). The rationale for performing this review was to provide a coordinated template on security and privacy from a technical perspective. For EHR systems, the objective was to investigate currently adopted EHR security and privacy technical features and reflect with the ISO/IEC 27002 and ISO/IEC 27001 standards (see Appendix Table 1A).

Method

We adopted the systematic literature review structure proposed by Kitchenham et al. and preferred reporting items for systematic reviews and meta-analysis (Liberati et al. 2009). The reporting of this paper follows PRISMA guidelines. The review protocol of our study has been published by Kitchenham (2004) and Kitchenham and Brereton (2013).

Eligibility criteria

Our inclusion criteria were full articles that dealt with the security and privacy of the technical implementations of EHR systems published in English in peer-reviewed journals and conference proceedings between 1998 and 2013. Our exclusion criteria were: literature surveys or informal literature surveys, letters, books and notes; articles solely discussing mobile health; and articles discussing only non-technical aspects of security and privacy in EHR systems.

Information sources

The search protocol was applied to Scopus and PubMed digital databases between January 1998 and December 2013, with defined search terms, including 'privacy', 'security', and 'electronic health record' OR 'electronic health record' OR 'EHR' OR 'personal health record' OR 'PHR' OR 'electronic patient record' OR 'EPR' OR 'PHI' OR 'electronic health' OR 'health exchange' OR 'patient record'.

Search and study selection

The search results identified 653 records with additional keywords including medical records, medical records systems, electronic medical records, medical information, and medical informatics (see Figure 1). We included 11 additional records through studies' references and removed four duplicate records from the 664 records and excluded 533 records based on inclusion and exclusion criteria. We then assessed the remaining 127 full text articles based on their titles, abstracts, keywords and conclusions. In total, 72 studies were excluded because they did not meet the objectives of the research question. Ultimately, the full text of 55 selected studies were reviewed in detail and categorised into a table (see Appendix Table 3A and Figure 1).

Data collection process

We collected the following data from each article: the author or authors, their country and institution; the year of publication; the source (journal or conference) of the study and reference; main scope, keywords, abstract, research questions and results; whether the study is a technical or non-technical work; and challenges, security implementation and privacy implementation. The current authors read each of the 55 papers independently; if opinions differed, FR made the final decision. Relevant data were extracted and managed through coding in NVivo, then compared in terms of the studies' focus on technical solutions.

Selection of quality studies

The quality assessment method presented in Kitchenham (2004) is based on CRD Guidelines (Khan et al. 2001) and the Cochrane reviewer's handbook (Deeks et al. 2003), in order to minimise study bias and maximise internal and external validity. It is important to assess the quality of primary studies to support the inclusion/exclusion process. We ensured that papers had acceptable quality and established quality criteria based on the completeness of data, and incomplete or irrelevant articles were eliminated based on the protocol. We identified quality criteria with a number of questions such as 'Did the study develop any technical solutions?', 'Did the study include any system/sample?' By quality appraisal of each primary study, we could determine the reliability of the sources and select quality studies prior to synthesis of results.

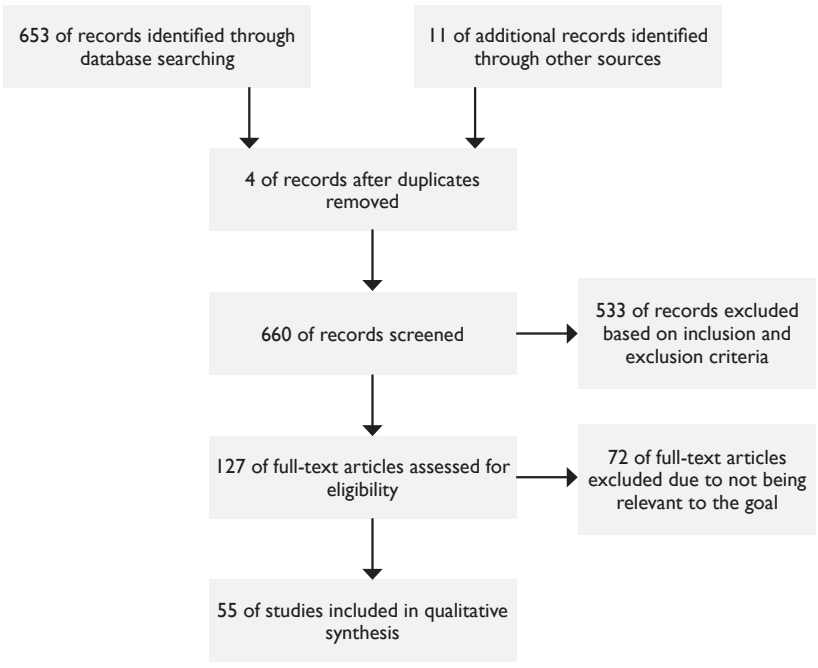

Figure 1: PRISMA flow diagram

We established a protocol during the planning phase because this is an important aspect of conducting secondary studies such as systematic reviews, in order to minimise bias. The protocol covered how the review was to be conducted, and included a detailed plan for the review, the process to be followed, and quality measures. The quality metrics applied to the primary studies and two of the authors were asked to assess the completeness of the review items. These observations led to some revisions to the protocol. We also appraised literature review results after inclusion and exclusion, step-based on the two journal rankings: SJR (SCImago 2012) and SNIP (CWTS Journal Indicators 2012), which have been provided by the Scopus digital database and CORE (CORE 2012) for conference proceedings. This appraisal showed that our review included approximately 89% of high quality journals (32 out of 36) and 26% (5 out of 19) of A to B ranked journals (Higgins, Altman & Sterne 2011).

Data items and synthesis of results

In the course of analysis, we used Nvivo software to store and systematically code the articles. We prepared a template of the security and privacy implementation of review articles as technical or non-technical and classified the following features: operations security, applicability, scalability, access control, cryptography, business continuity , communication security, consistency and continuity, accuracy and quality, data breach notification, fault tolerance, flexibility, interoperability, key management, maintenance and retrieval service, privacy safeguarding, non-repudiation, consent and choice mechanism, policies and regulations, security checks and updates, integration, sharing, compliance. In light of the fact that we appraised technical articles based on the research question, administrative papers were not included. These features were selected based on the review articles' objectives. Then, in accordance with the frequently adopted security and privacy requirements in review articles and our research objective, we selected 13 technical features that were highly cited and applied in EHR systems which we elaborate in the results section. Table 1A (Appendix) shows the number of articles that cited relevant features and whether or not the selected ISO standards contain those.

Results

Our results are presented according to privacy and security characteristics that are summarised in Table 3A (Appendix).

System and application access control

Defining access control strategies and policies is imperative in order to ensure security of EHR systems. Access control should be well addressed to provide confidentiality by limiting the access rights of system users to patient data and assigning the proper access rights by establishing the system Access Control List (ACL). This can be done by access control mechanisms such as broker-based access control. Furthermore, when the database contains personally identifiable information, access control can be employed in order to provide privacy with only authorised parties able to access (Bouhaddou et al. 2012; Chen, Lu & Jan 2012; Murray, Calhoun & Philipsen 2011; van der Haak et al. 2003; Wu, Ahn & Hu 2012). There are different types of access control models, including: Role-Based Access Control (RBAC), Attribute-Based Access Control (ABAC) and Cryptographic Access Control (CAC) (Blobel & Pharow 2007; Bouhaddou et al. 2012; Martínez, Sánchez & Valls 2013). The role-based and time-bound access controls provides flexibility of roles to control the access of health information with respect to the time dimension (Zhang et al. 2011). However, ABAC is used more frequently than RBAC in EHR systems due to its flexibility in the policy descriptions (Singh, Gupta & Mohan 2013). XACML is an open standard of access control policy language, which has been used in many articles to define access control polices (Hsieh & Chen 2012).

Secure communication

A secure communication channel needs to be established before exchanging EHR data with some mechanisms such as firewalls (Acharya et al. 2013; Liu et al. 2012; Mackenzie et al. 2011; Tsai 2010; van der Haak et al. 2003), VPN (Acharya et al. 2013; Aljarullah & El-Masri 2012; Blobel & Roger-France 2001; Li et al. 2011; Mackenzie et al. 2011; van der Haak et al. 2003), network segregation (Acharya et al. 2013), and SSL/TLS (Acharya et al. 2013; Bakers & Masys 1999; Blobel & Roger-France 2001; Guo et al. 2012; Li et al. 2011; Safran & Goldberg 2000; Stingl & Slamanig 2011; von Laszewski, Dayal & Wang 2011; Zhang & Liu 2010). The eTRON architecture described in Khan & Sakamura (2012) uses secure communication by proposing an authentication scheme and hybrid access control model. Therefore, encrypting the communication channel can be applied in order to provide authentication, integrity, confidentiality, non-repudiation and accountability of EHR exchange. In addition, the secure communication channels have been addressed by many applicable standards, such as HL7, EDIFACT, xDT, and XACML (Afzal et al. 2011; Bakers & Masys 1999; Blobel & Roger-France 2001; Bouhaddou et al. 2012; Barber 1998; Li et al. 2011; Murray, Calhoun & Philipsen 2011; Santos et al. 2011; Tsai 2010). The HL7 specifies standards, guidelines and methodologies to provide a framework for the exchange, integration, sharing, and retrieval of electronic health information or secure message delivery (SMD) which are the dominant health messaging standards used in the USA, Canada, Holland, Germany, Australia, and New Zealand and are being adopted by other countries as well (Standards Australia 2013; Health Level Seven International 2013).

Compliance with security requirements

EHR systems implementations should comply with security requirements and standards such as HIPAA, HL7, eXtensible Access Control Markup Language, CORBA, CEN ENV 13606, GEHR/open EHR, MML standard, HITECH guidance, and ISO EHR standards. Healthcare vendors should adhere to agreed vocabularies (Bouhaddou et al. 2012) and healthcare providers should consider common standards that can enable EHR data exchange efficiently (Afzal et al. 2011; Zhang & Liu 2010). In total, 21 and 19 articles respectively indicated the compliance with HIPAA and HL7 standards, which demonstrate the importance of establishing common platforms. HIPAA provides guidelines to protect privacy and security of health information (Acharya et al. 2013). HL7 (Health Level Seven International 2013) specifies the structure of health information and provides a framework for information exchange (Singh et al. 2013).

Interoperability

Interoperability is a feature that enables information systems to exchange information, thereby enhancing the availability of information. Interoperability demands information security, including restriction of unauthorised access, use, disclosure and modification of data, in order to ensure confidentiality, integrity and availability. According to the main goal of Health Information Exchange (HIE) systems, semantic interoperability is a significant issue in the integration of EHR data in different repositories, and the review articles proposed different methods to provide such interoperability. Policies, such as CEN prENV 1306 policy, required mandating and formulating to be able to provide interoperability (Blobel & Pharow 2007; Barber 1998). The Data Segmentation for Privacy (DS4P) (Coleman 2013) aims at ensuring semantic interoperability by using standards to handle health information across different systems, such as HIE architecture designed by Afzal et al. (2011) which is based on HL7 V3 standard messaging to provide high interoperability. eMOLST provides interoperability

based on Integrating Healthcare Enterprises (IHE) among health record systems in large scale sharing with Security Assertion Markup Language (SAML) (von Laszewski, Dayal & Wang 2011). In addition, application of Continuity of Care Documents (CCD) can enhance interoperability and portability (Hsieh & Chen 2012). Broker-based composite EHR authorisation provides interoperability by establishing a small system, and then the Health Information System Broker (HISB) organises the patient data in the local and public databases (Aljarullah & El-Masri 2012). In the global Dolphin Project (Li et al. 2011) the interoperable EHR is achieved by encapsulated and modularised applications, which can be transformed into Service Oriented Architecture (SOA) with the implementation of security requirements. The bIT4 health project (Blobel & Pharow 2007) presented a telematics platform to provide semantic interoperability through formal Computation Independent Models (CIM).

Consent and choice mechanism

There are increasing demands for allowing patients to have control over their data in order to be able to decide who can have access to their sensitive health information and to share their EHR information with national clinical research networks. Canada Health Infoway in Privacy and Security Architecture (PSA) recommended access control mechanisms including DAC and RBAC to provide patient consent (Khan & Sakamura 2012). In addition, in the EU FP7 project (PONTE), hospitals are responsible for informing patients and obtaining their consent before disclosing their data. Written patient consent is necessary for data protection agreements (van der Haak et al. 2003). However, as has been defined by privacy legislations such as HIPAA privacy rule, Data Privacy Rule UK, NSW Health Record Information Privacy Act and other legislations, health professionals can access patient data without explicit consent in medical emergencies (Win & Fulcher 2007; Win 2005; Sun et al. 2011), and the healthcare provider is not forced to obtain patient consent to use or disclose such data for payment, treatment or healthcare operations (Murray, Calhoun & Philipsen 2011). The Digital Rights Management technique helps to provide patient consent in EHR systems (Chen, Lu & Jan 2012). A series of ISO standards, including ISO/DTS 17975 and ISO/TS 27790:2009, supply patient consent by privacy related profiles and techniques such as Patient Identification Cross-Referencing (PIX) and Cross-Enterprise User Assertion (XUA). The Data Segmentation for Privacy (DS4P) initiative supports privacy policies for health information sharing and enables health information technology systems to implement privacy protection requirements (Coleman 2013).

Policies and regulations

Security and privacy policies and regulations discussed in articles reviewed include different types, such as access control policies, authorisation policies, delegation policies, governing policies and regulations, disclosure policies, sharing and integrating policies and medical regulations. Policy has been defined as the 'legal frameworks about rules and regulations, organizational and administrative frameworks, functionalities, claims and objectives involving principles, agreements, rights, penalties and duties along with technical solutions for processing and communicating information systems' (Blobel 2004: pp.251-257). Robust policies and procedures can help to achieve high level security and privacy (Guo et al. 2012; Matteucci et al. 2011; Zhang & Liu 2010). Enacting common policies and regulations can facilitate the sharing of health information (Afzal et al. 2011; Huang, Lee & Lee 2012; Bouhaddou et al. 2012).

Flexibility

Applying role-based and time-bound access control can provide flexibility in EHRs (von Laszewski, Dayal & Wang 2011). However, Attribute-Based Access Control (ABAC) is more desirable than Role-Based Access Control (RBAC) in EHR systems due to its features of flexibility and granularity in the policy descriptions (Safran & Goldberg 2000). In addition, proper network architecture establishment across different EHR data systems, such as three-tier architectures, can enhance flexibility and scalability features of EHR systems with a higher level of security (Toh et al. 2011). The scalability is important to large distributed EHR systems for handling greater amounts of data (Aljarullah & El-Masri 2012; Li et al. 2011). A flexibility feature is required in defining the security policies concerning the automatic decision making in medical emergencies (Li et al. 2013) and distributed EHR systems leading to interoperability among systems for health information exchange (Blobel & Pharow 2006).

Applicability and scalability

One of the objectives of an EHR system in private and public domains, is that EHR systems, by providing applicability and scalability features, should support patients, thereby enabling them to have access to their data outside home and especially in medical emergencies (Li et al. 2013; Zhang et al. 2011). Applicability of privacy and security rules to EHR systems implementation are crucial for EHR disclosure (Burton et al. 2013). Also, scalability of EHR systems evolves into

the large size and complexity of the system operation which should be ensured in storage, computation, key management and communication of the EHR system (Li et al. 2013). To provide scalability in the cloud computing environment, a fine-grained access control scheme could be applied as one of the solutions in an EHR based encryption technique.

Integration and sharing

Despite many advances in the cloud computing environment and Personal Health Record (PHR) services in the provision of EHR integration and sharing, there are barriers to secure storage, usage, and access management of data (Chen, Lu & Jan 2012; Chen et al. 2012; Singh, Gupta & Mohan 2013; Wu, Ahn & Hu 2012; Zhang & Liu 2010; Rodrigues et al. 2013). There are two important aspects which need to be addressed in EHR sharing: 'authenticity and integrity of EHR' and 'not integrating EHRs with non-legitimate or untrustworthy EHR owners'. Matteucci et al. (2011) suggest 'data sharing policies' to enable EHR data sharing with a controlled natural language called CNL4DSA, which can assure confidentiality and integrity. Healthcare Interchange Exchange (HIE) can link different nations to share health information by providing a unified interface to various stakeholders (Afzal et al. 2011). The implementation of a national EHR system using a semi-centralised or centralised approach can aggregate EHRs from different systems, and this enhances the quality and controls the costs (Baldas, Giokas & Koutsouris 2010). This has been adopted in some countries, such as Canada, Australia, Denmark, Finland, England, India and Estonia.

Cryptography techniques

Cryptography techniques can ensure confidentiality, integrity, non-repudiation, authentication, and authorisation, which can be classified into cryptography on the server, user and the transmission sides. Digital signatures can provide patient privacy with the aid of a Trusted Third Party (TTP) to investigate any unusual medical transactions and prevent illegal and unauthorised activities. The Certificate Authority (CA) is a TTP, which issues certificates and offers services such as 'keeping public keys, offering directory service, and issuing certificates' (Hsiao et al. 2012). End-to-end encryption (E2EE), authentication and authorisation may satisfy the basic security requirements in the lower levels with access control policies in the higher levels (Singh et al. 2013). Moreover, pseudonymisation such as PIPE (Pseudonymization of Information for Privacy in E-health) framework and anonymisation can provide confidentiality and privacy in health record systems (Neubauer & Heurix 2011). Key management issues such as storing, updating, and revoking are crucial aspects to be considered in cryptography (Li et al. 2013). Ciphertext-Policy ABE (CP-ABE) or Public-Key Encryption (PKE) with keyword search schemes provides patient controlled encryption and privacy keyword search especially in fine-grained integrated systems (Hsieh & Chen 2012).

Business continuity techniques

Business continuity includes the utility and availability of EHR systems. The EHR systems must be instantly available when required and security controls need to be applied to protect health information and communication channels in cooperating EHR systems to preventing any disruptions or failures (Chen, Lu & Jan 2012; van der Haak et al. 2003). The availability of patient data can be implemented with security technologies, such as digital clustering, RAID systems and back-up procedures (van der Haak et al. 2003). Utility means the system usability based on security implementation, and privacy and security establishments (Aljarullah & El-Masri 2012; Chen, Lu & Jan 2012; Chen et al. 2012; Stingl & Slamanig 2011; Sun et al. 2011; Tsai 2010; van der Haak et al. 2003; Zhang & Liu 2010). Cloud computing designs can help provide a high level of availability and utility of EHR information (Aljarullah & El-Masri 2012; Chen et al. 2012; Hsieh & Chen 2012; Huang et al. 2013; Li et al. 2013; Singh et al. 2013; Stingl & Slamanig 2011).

Accuracy and quality

Providing accuracy and quality features are priorities for better EHR system services, which lead to security and privacy protection of EHR data. Integrity protection provides accuracy and consistency for data in EHR systems (Bakers & Masys 1999; Chen, Lu & Jan 2012; Huang et al. 2013; Riedl & Grascher 2010; Zhang & Liu 2010). The PCASSO project (Patient-centered access to secure systems online) improves the quality of care and provides confidentiality and privacy of patient data by applying proper security techniques including RBAC, multi-level security, authentication, encryption and audit trails (Bakers & Masys 1999). By implementing a 'quality assurance plan' (Hunter 2013), health plans can be monitored to report any data breaches and provide the security and confidentiality of EHR transactions.

Operations security

Operations security includes monitoring, audit, archiving, and back-up in EHR systems. Audit refers to record logs of users' activities. Archiving means to store information in an offline site to be able to restore them when necessary (Chen, Lu & Jan 2012; Zhang &

Liu 2010). Monitoring is significant in order to provide security of data transmission through communication channels, identify any suspicious activity and respond to any malicious events. Intrusion Detection and Prevention Systems (IDPS) is one such system (Acharya et al. 2013; Mackenzie et al. 2011; Sun et al. 2011; Toh et al. 2011). The EHR system should offer mechanisms to back-up patient data for authorised users to ensure patient privacy (Stingl & Slamanig 2011).

Discussion

In this section we discuss our main findings, and compare our results with ISO/IEC 27002 (ISO 2013) and ISO/IEC 27002 (ISO 2011) standards that are summarised in Tables 1A and 3A (Appendix).

Access control policies and restrictions need to be defined through proper standards such as ISO standards in order to secure the EHR systems, before establishing any access control application. Enacting appropriate standards and procedures, secure methods to design an efficient encryption scheme and key management have been highlighted by research results. Applying the cryptographic controls in policies and key management achieve information security goals, including confidentiality, integrity, authenticity, non-repudiation, and authentication.

The review studies showed that EHR system implementations require planning for secure communication. Encrypting the communication channel with defining the proper standards and regulations pertaining to data exchange, such as HL7, HITECH, HEASNET can ensure secure health data exchange in clinical networks. Networks have to be managed and controlled by proper implementations to protect and provide security of information and prevent unauthorised access. The appropriate security and privacy procedures can increase reliability and particularly security of EHR systems.

Our study findings demonstrated the existence of gaps in the interoperability requirement of information systems to provide meaningful use, security and privacy for data exchange. Interoperability of EHR systems can facilitate data access, data retrieval, and provide a secure and efficient system. To address interoperability, applications have to adhere to acceptable formats, regulations, and standards.

The choice principles include providing explicit, understandable, affordable and accessible mechanisms to give consent to the user in accessing their data at the collection time. Our study findings reveal the existing gaps in providing patient consent concerning defined policies and guidelines that need to be considered in future studies. Concerning patient consent, our findings suggested that patients' control over their data to grant access to authorised users and share data to clinical research networks should follow the standard's guidelines based on specific location. Patient consent means informing the user in processing their personal information except where they cannot freely withhold consent. Moreover, healthcare providers should inform patients before obtaining the opt-in or opt-out user consent method in processing their information, and inform users about their rights: participation and access rights.

To provide flexibility in EHR systems, the review articles suggested solutions such as implementing security and privacy policies, and appropriate architectures. Our appraisal reveals existing gaps in selected ISO standards concerning flexibility features of EHR systems. The flexibility feature is significant in defining security policies in order to service distributed and interoperable EHR systems. Applicability and scalability in designing EHR systems can be ensured with cryptography techniques, proper exchange platforms, and privacy policies to enhance security and privacy of EHRs. Fine-grained access control in review studies has been proposed as one solution which can ameliorate the applicability and scalability in EHR systems expansion.

Our study findings suggest that there is a demand for standards to emphasise security and privacy protection when dealing with system sharing. Information sharing agreements need to be established to improve the coordination of security implementation. Therefore, security requirements must be defined in the agreements. For sharing or integrating EHRs, healthcare providers need to highlight comprehensive guidelines across different systems. Notably, applicable guidelines and techniques for EHR systems, such as proper encryption schemes and access control mechanisms need to be included.

In our view, for the provision of security and privacy in EHR systems there needs to be greater emphasis on the application of security operations, including documented operating procedures, controls against malwares, technical vulnerability management, control of operational software, and checks and updates. This was not always the case in the reviewed literature.

Business continuity includes utility and availability of EHR systems along with appropriate security protections. Business continuity can be ensured by establishing processes, procedures and controls for providing the availability of the system under adverse conditions. Redundancy requirements should be considered to meet the availability of information systems.

Our study findings suggest addressing accuracy and quality feature in EHR systems to provide better services, quality of care, confidentiality and patient privacy, which are covered in both standards. It defines accuracy and quality as correctness, completeness of personal information, adequate and relevant purpose of use, reliability, establishing collection procedures and control mechanisms. To secure communication our study findings suggest considering the management of networking, operational responsibility of networks, safeguarding of confidentiality and integrity, appropriate logging and monitoring, management of activities, authentication and restrictions.

The legal and contractual compliance requirements include guidelines to protect intellectual property and avoid legal or regulatory breaches of data security requirements. The information security policies including management direction, policies and reviews direct the technical requirements of the system. Information security reviews should be utilised for analysing the compliance of information processing and procedures, which we believe should be approached by EHR systems. Owing to the increasing demands and growing complexity of ICT systems, there are difficulties in ensuring privacy and adherence to laws. In addition, privacy policies should provide applicability for 'privacy safeguarding requirements'. Robust and common policies and procedures can help to achieve high level security and privacy and can facilitate the sharing and exchanging of health information.

Study limitations

In this study, we consider securing EHR systems from a technical perspective. However, organisational and administrative perspectives also play important roles in securing EHRs, as administrative policies and procedures drive the requirements and technical perspectives that will address these issues. Therefore, sociotechnical perspectives such as consent mechanisms and business continuity aspects should not be ignored. Review articles were selected based on the search protocol, and specific study selection, data collection and appraisal processes have not been considered. Although 16 out of 55 articles comply with HIPAA standards that are US-centric, the remaining articles focus on EHR technical perspectives in general. Other limitations of the study include removal of survey and mobile healthcare studies that focused merely on mobile networking. In addition, the researchers did not include articles published after the search date; they selected two relevant and available information security ISO standards; and the study's main focus was on technical rather than physical or organisational perspectives.

Conclusions

In summary, our study was undertaken to investigate crucial technical security and privacy requirements of EHR systems based on a comparison of a systematic review of the literature with ISO/IEC 27002:2013 and ISO/IEC 29100:2011 standards. Our findings demonstrate, regardless of the enormous effort required, well defined access control policies should be mandated in order to provide patient privacy by limiting the access rights to patient data with proper access control policy languages and standards. Applicability of privacy and security rules and scalability of EHR system implementations can be provided with proper architectures and frameworks, cryptography techniques and policies. EHR systems implementation should comply with security requirements and standards; then information processing and procedures to EHR systems should be analysed and monitored with information security review plans. EHR system sharing and integration requirements need to be addressed by standards and applicable guidelines through security implementations. In addition, there are increasing demands to provide patients' consent with well-defined policies and guidelines and access control mechanisms that can authorise patients and healthcare system users to share their records with clinical networks. The interoperability feature of EHR systems can facilitate health information exchange, data access and data retrieval, which need to adhere to acceptable formats, regulations and standards. Availability and utility of EHR systems should be provided with security operations including redundancy, management of networking, operational responsibility of networks, safeguarding integrity and confidentiality, monitoring and logging, authentication and restrictions for secure communications. Accuracy, quality and flexibility features in EHR systems must be ensured in order to provide better EHR system services and quality of care.

Acknowledgements

The authors gratefully acknowledge Professor Yi Mu for his invaluable comments in preparing this paper and the help of Dr. Madeleine Strong Cincotta in the language editing.

References

Acharya, S., Coats, B., Saluja, A. and Fuller, D. (2013). Secure electronic health record exchange: achieving the meaningful use objectives. *46th Hawaii International Conference on System Sciences*. Wailea, Hawaii, USA, 2555-2564. Available at: http://www.computer.org/csdl/proceedings/hicss/2013/4892/00/4892c555.pdf (accessed 23 August 2013).

Afzal, M., Hussain, M., Ahmad, M. and Anwar, Z. (2011). Trusted framework for health information exchange. *Frontiers of Information Technology*, Islamabad. Available at: http://www.computer.org/csdl/proceedings/fit/2011/4625/00/4625a308.pdf (accessed 23 August 2013).

Aljarullah, A. and El-Masri, S. (2012). A novel system architecture for the national integration of electronic health records: a semi-centralized approach. *Journal of Medical Systems* 37(4): 9953.

Bakers, D.B. and Masys, D.R. (1999). PCASSO: a design for secure communication of personal health information via the internet. *International Journal of Medical Informatics* 54(2): 97-104.

Baldas, V., Giokas, K. and Koutsouris, D. (2010). Multilevel access control in hospital information systems. *IFMBE Proceedings: XII Mediterranean Conference on Medical and Biological Engineering and Computing,* Berlin. Available at: http://link.springer.com/search?query=Multilevel+access&search-within=Book&facet-book-doi=10.1007%2F978-3-642-13039-7 (accessed 23 August 2013).

Barber, B. (1998). Patient data and security: an overview. *International Journal of Medical Informatics* 49(1): 19-30.

Blobel, B. (2000). Advanced tool kits for EPR security. *International Journal of Medical Informatics*, 60(2):169-175.

Blobel, B. and Roger-France, F. (2001). A systematic approach for analysis and design of secure health information systems. *International Journal of Medical Informatics* 62(1): 51-78.

Blobel, B. (2004). Authorization and access control for electronic health record systems. *International Journal of Medical Informatics* 73(3):251-257.

Blobel, B. and Pharow, P. (2007). A model driven approach for the German health telematics architectural framework and security infrastructure. *International Journal of Medical Informatics* 76(2-3): 169-175.

Blobel, B. and Pharow, P. (2006). Formal policies for flexible EHR security. *Studies in Health Technology and Informatics* 121: 307-316.

Blythe, M.J. et al. (2012). Standards for health information technology to ensure adolescent privacy. *Pediatrics* 130(5): 987-990.

Bouhaddou, O., Cromwell, T., Davis, M., Maulden, S., Hsing, N., Carlson, D., Cockle, J., Hoang, C. and Fischetti, L. (2012). Translating standards into practice: experience and lessons learned at the Department of Veterans Affairs. *Journal of Biomedical Informatics* 45(4): 813-823.

Botella, F., Alarcon, E. and Penalver, A. (2013). A new proposal for improving heuristic evaluation reports performed by novice evaluators.72-75, Chile. Available at: http://dl.acm.org/results.cfm?h=1&cfid=647993084&cftoken=61477287 (accessed 20 March 2013).

Burton, B., Cothran, C., Davis, N., Dooling, J., Dunn, R., Jensen, J., Odia, G., Rose, A. D. and Twiggs, M. (2013). The privacy and security of occupational health records. *Journal of AHIMA / American Health Information Management Association* 84(4): 52-56.

Chen, Y.Y., Lu, J.C. and Jan, J.K. (2012). A secure EHR system based on hybrid clouds. *Journal of Medical Systems* 36(5): 3375-3384.

Chen, T.S., Liu, C.H., Chen, T.L., Chen, C.S., Bau, J.G. and Lin, T.C. (2012). Secure dynamic access control scheme of PHR in cloud computing. *Journal of Medical Systems* 36(6): 4005-4020.

Coleman, J. (2013). Segmenting data privacy. Cross-industry initiative aims to piece out privacy within the health record. *Journal of AHIMA/ American Health Information Management Association* 84(2): 34-38.

CORE (2012). *The CORE Conference Ranking Exercise*. Available at: www.core.edu.au/coreportal (accessed 8 December 2013).

CWTS Journal Indicators (2012). *SNIP indicator*. Available at: http://www.journalindicators.com (accessed 8 December 2013).

Deeks, J., Higgins, J., and Altman, D. (2003). *Cochrane Reviewers' Handbook 4.2.1*. The Cochrane Library. Chichester, John Wiley & Sons Ltd.

De Oliveira, K.S. and Soares, M.S. (2012). A systematic review on aspects in software architecture design. *International Conference of the Chilean Computer Science Society,* 21-28, Valparaiso. Available: http://www.computer.org/csdl/proceedings/sccc/2012/2938/00/2937a021.pdf (accessed 20 March 2013).

Dos Santos, A.C.C, Delamaro, M.E. and Nunes, F.L.S. (2013). The relationship between requirements engineering and virtual reality systems: A systematic literature review. XV *Symposium on Virtual and Augmented Reality*: 53-62. Cuiaba. Available at: http://dl.acm.org/citation.cfm?id=2511560 (accessed 20 March 2013).

Fernández-Alemán, J. L., Señor, I. C., Lozoya, P. T. O. and Toval, A. (2013). Security and privacy in electronic health records: a systematic literature review. *Journal of Biomedical Informatics* 46(3): 541-562.

Flores Zuniga, A.E., Win, K.T. and Susilo, W. (2010). Functionalities of free and open electronic health record systems. *International Journal of Technology Assessment in Health Care* 26(4): 382-389.

Guo, L. Liu, X. Fang, Y. and Li, X. (2012).User-centric private matching for eHealth networks - a social perspective. *Globecom 2012 IEEE - Communication and Information System Security Symposium*, Anaheim, California. Available at: IEEE Xplore, http:// www.ieee.org (accessed 23 August 2013).

Higgins, J., Altman, D.G. and Sterne, J.A.C. (Eds) (2011). Chapter 8: Assessing risk of bias in included studies. In: *Cochrane Handbook for Systematic Reviews of Interventions Version 5.1.0* [updated March 2011]. J. Higgins & S. Green (Eds). Available at: http://www.cochrane-handbook.org (accessed 13 April 2015).

Health Level Seven International (HL7) (2013). *Introduction to HL7standards.* Available at: http://www.hl7.org/implement/standards/ (accessed 5 January 2014).

Hsiao, T.C., Wu, Z.Y., Chung, Y.F., Chen, T.S. and Horng, G.B. (2012). A secure integrated medical information system. *Journal of Medical Systems* 36(5): 3103-3113.

Hsieh, G. and Chen, R.J. (2012). Design for a secure interoperable cloud-based Personal Health Record service. *IEEE 4th International Conference on Cloud Computing Technology and Science*, Taipei. Available at: IEEE Xplore, http:// www.ieee.org (accessed 23 Aug. 2013).

Huang, C., Lee, H. and Lee, D.H. (2012). A privacy-strengthened scheme for e-healthcare monitoring systems. *Journal of Medical Systems* 36(5): 2959-2971.

Huang, J., Sharaf, M. and Huang, C.T. (2013). A hierarchical framework for secure and scalable EHR sharing and access control in multi-cloud. *41st International Conference on Parallel Processing Workshops*, Pittsburgh, Pennsylvania, USA. Available at: IEEE Xplore, http:// www.ieee.org (accessed 23 August 2013).

Hunter, E.S. (2013). Electronic health records in an occupational health setting - Part I. A global overview. *Workplace Health and Safety* 61(2): 57-60.

ISO (2013). *ISO/IEC 27002 Information technology — Security techniques — Code of practice for information security controls*. Available at: http://www.iso.org/iso/home.html (accessed 2 December 2013)

ISO (2011). *ISO/IEC 29100 Information technology — Security techniques — Privacy framework*, Available at: http://www.iso.org/iso/home.html (accessed 2 December 2013).

ISO (2008). *ISO 27799 Information security management in health using ISO/IEC 27002,* Available at: http://www.iso.org/iso/home.html (accessed 15 March 2013).

Khansa, L., Forcade, J., Nambari, G., Parasuraman, S. and Cox, P. (2012). Proposing an intelligent cloud-based electronic health record system. *International Journal of Business Data Communications and Networking* 8(3): 57-71.

Khan, M.F.F. and Sakamura, K. (2012). Security in healthcare informatics: design and implementation of a robust authentication and a hybrid access control mechanism. *The 5th International Conference on Communications, Computers and Applications (MIC-CCA2012),* Istanbul, Turkey. Available at: IEEE Xplore, http:// www.ieee.org (accessed 23 August 2013).

Khan, K. S., Ter Riet, G., Glanville, J., Sowden, A. J. and Kleijnen, J. (2001). *Undertaking systematic reviews of research on effectiveness: CRD's guidance for carrying out or commissioning reviews* No. 4 (2nd ed.). NHS Centre for Reviews and Dissemination.

Kitchenham, B.A., Pearl Brereton, O., Budgen, D., Turner, M., Bailey, J. and Linkman, S. (2009). Systematic literature reviews in software engineering: a systematic literature review. *Information and Software Technology* 51(1): 7-15.

Kitchenham, B.A. (2004). *Procedures for performing systematic reviews.* Technical Report TR/SE-0401. Keele, UK, Keele University NICTA Technical Report 0400011T.1.

Kitchenham, B.A. and Brereton, P. (2013). A systematic review of systematic review process research in software engineering. *Information and Software Technology* 55(12): 2049-2075.

Liberati, A., Altman, D. G., Tetzlaff, J., Mulrow, C., Gøtzsche, P. C., Ioannidis, J. P., et al. (2009). The PRISMA statement for reporting systematic reviews and meta-analyses of studies that evaluate health care interventions: explanation and elaboration. *Annals of Internal Medicine* 151(4): W-65-W-94.

Liu, C.H., Chung, Y.F., Chen, T.S. and Wang, S.D. (2012). The enhancement of security in healthcare information systems. *Journal of Medical Systems* 36(3): 1673-1688.

Li, J. S., Zhou, T. S., Chu, J. Araki, K. and Yoshihara, H. (2011). Design and development of an international clinical data exchange system: the international layer function of the Dolphin Project. *Journal of the American Medical Informatics Association* 18(5): 683-689.

Lee, T.F., Chang, I.-P. and Wang, C.C. (2013). Simple group password-based authenticated key agreements for the integrated EPR information system. *Journal of Medical Systems* 37(2).

Li, M., Yu, S., Zheng, Y., Ren, K. and Lou, W. (2013). Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption. *IEEE Transactions on Parallel and Distributed Systems* 24(1): 131-143. Available at: IEEE Xplore, http:// www.ieee.org (accessed 23 August 2013).

Mackenzie, I.S., Mantay, B.J., McDonnell, P. G., Wei, L. and Macdonald, T. M. (2011). Managing security and privacy concerns over data storage in healthcare research. *Pharmacoepidemiology and Drug Safety* 20(8): 885-893.

Martínez, S., Sánchez, D. and Valls, A. (2013). A semantic framework to protect the privacy of electronic health records with non-numerical attributes. *Journal of Biomedical Informatics* 46(2): 294-303.

Matteucci, I., Mori, P., Petrocchi, M. and Wiegand, L. (2011). Controlled data sharing in e-health. *1st Workshop on Socio-Technical Aspects in Security and Trust (STAST),* Milan. Available at: IEEE Xplore, http:// www.ieee.org (accessed 23 August 2013).

Moher D., Liberati A., Tetzlaff J. and Altman D.G. (2009). The PRISMA Group. Preferred Reporting Items for Systematic Reviews and Meta-Analyses: The PRISMA Statement. *PLoS Med* 6(6): e1000097. doi:10.1371/journal.pmed1000097.

Murray, T.L., Calhoun, M. and Philipsen, N.C. (2011). Privacy, confidentiality, HIPAA, and HITECH: Implications for the health care practitioner. *Journal for Nurse Practitioners* 7(9): 747-752.

Murphy, S.N., Gainer, V., Mendis, M., Churchill, S. and Kohane, I. (2011). Strategies for maintaining patient privacy in i2b2. *Journal of the American Medical Informatics Association* 18(1): 103-108.

Neubauer, T. and Heurix, J. (2011). A methodology for the pseudonymization of medical data. *International Journal of Medical Informatics* 80(3): 190-204.

Pantazos, K., Lauesen, S. and Lippert, S. (2011). De-identifying an EHR database-anonymity, correctness and readability of the medical record. *Studies in health technology and informatics* 169: 862-6.

Riedl, B. and Grascher, V. (2010). Assuring integrity and confidentiality for pseudonymized health data. *International conference on Electrical Engineering/ Electronics Computer Telecommunications and Information Technology (ECTI-CON)*, Chiang Mai, Thailand. Available at: IEEE Xplore, http:// www.ieee.org (accessed 23 August 2013).

Rodrigues, J.J.P.C., De La Torre, I., Fernández, G. and López-Coronado, M. (2013). Analysis of the security and privacy requirements of cloud-based electronic health records systems. *Journal of Medical Internet Research* 15(8): e186.

Safran, C. and Goldberg, H. (2000) Electronic patient records and the impact of the Internet. *International Journal of Medical Informatics* 60(2): 77-83.

Sahama T. and Miller, E. (2011). Informed use of patients' records on trusted health care services. *International Perspectives in Health Informatics*, Victoria, British Columbia, Canada.

Santos, J., Pedrosa, T., Costa, C. and Oliveira, J. (2010). *Modeling a portable personal health record.* Proceedings of the Third International Conference on Health Informatics, 20-23 January 2010, Valencia, Spain.

Santos, C., Pedrosa, T., Costa, C. and Oliveira, J. L. (2011). *On the use of openEHR in a portable PHR.* HEALTHINF-Proceedings of the International Conference on Health Informatics, Rome, Italy. Available at: BibSonomy, http:// www.bibsonomy.org (accessed 23 August 2013).

SCImago (2012). SJR — *SCImago Journal & Country Rank*. Available at: http://www.scimagojr.com (accessed 8 December2013).

Singh, R., Gupta, V. and Mohan, K. (2013). Dynamic federation in identity management for securing and sharing personal health records in a patient centric model in cloud. *International Journal of Engineering and Technology* 5(3): 2201-2209.

Standards Australia (2013). *Health Level 7 (HL7)* Available at: http://www.ehealth.standards.org.au/StandardsOrganisations/HealthLevel7.aspx (accessed 2 January 2014).

Stauch, M., Forgó, N. and Krügel, T. (2013). Using EHRs to design drug repositioning trials: A devolved approach to data protection. *International Review of Law, Computers and Technology*, 01 July 2013.

Stingl, C. and Slamanig, D. (2011). Health records and the cloud computing paradigm from a privacy perspective. *Journal of Healthcare Engineering* 2(4): 487-508.

Sun, J., Zhu, X., Zhang, C. and Fang, Y. (2011). HCPP: Cryptography based secure EHR system for patient privacy and emergency healthcare. *31st International Conference on Distributed Computing Systems*, Minneapolis, MN. Available at: IEEE Xplore, http:// www.ieee.org (accessed 23 August 2013).

Tharaud, J., Wohlgemuth, S., Echizen, I., Sonehara, N., Müller, G. and Lafourcade, P. (2010). Privacy by data provenance with digital watermarking: A proof-of-concept implementation for medical services with electronic health records. *Sixth International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP)*, Darmstadt. Available: IEEE Xplore, http:// www.ieee.org (accessed: 23 August 2013).

Toh, S., Platt, R., Steiner, J.F. and Brown, J.S. (2011). Comparative-effectiveness research in distributed health data networks. *Clinical Pharmacology and Therapeutics* 90(6): 883-887.

Tsai, F.S. (2010). Security issues in e-healthcare. *Journal of Medical and Biological Engineering* 30(4): 209-214.

van der Haak, M., Wolff, A.C., Brandner, R., Drings, P., Wannenmacher, M. and Wetter, Th. (2003). Data security and protection in cross-institutional electronic patient records. *International Journal of Medical Informatics* 70(2-3): 117-130.

Von Laszewski, G., Dayal, J. and Wang, L. (2011). EMOLST: A documentation flow for distributed health informatics. *Concurrency and Computation: Practice and Experience* 23(16): 1857-1867.

Wickboldt, A.K. and Piramuthu, S. (2012). Patient safety through RFID: Vulnerabilities in recently proposed grouping protocols. *Journal of Medical Systems* 36(2): 431-435.

Win K.T. and Fulcher J. (2007), Consent mechanisms for electronic health record systems: a simple yet unresolved issue. *Journal of Medical Systems* 31(2): 91-96.

Win K.T. (2005). A review of security of electronic health record systems. *Health Information Management Journal* 34(1): 13-18.

Wu, C.H., Hwang, J.J. and Zhuang, Z.Y. (2013). A trusted and efficient cloud computing service with personal health record. *International Conference on Information Science and Applications (ICISA) Suwon*, Korea (South). Available at: IEEE Xplore, http:// www.ieee.org (accessed 23 August 2013.

Wu, R., Ahn, G.J. and Hu, H. (2012). Secure sharing of electronic health records in clouds. *8th International Conference on Collaborative Computing: Networking, Applications and Worksharing (CollaborateCom)*, Pittsburgh, Pennsylvania. Available at: IEEE Xplore, http:// www.ieee.org (accessed 23 August 2013).

Zhang R. and Liu, L. (2010). Security models and requirements for healthcare application clouds. *IEEE 3rd International Conference on Cloud Computing*, Miami, Florida. Available at: IEEE Xplore, http:// www.ieee.org (accessed 23 August 2013).

Zhang, R., Liu, J., Han, Z. and Liu, L. (2011). RBTBAC: Secure access and management of EHR data. *International Conference on Information Society (i-Society)*, London. Available at: IEEE Xplore, http:// www.ieee.org (accessed 23 August 2013).

Corresponding author:

Fatemeh Rezaeibagha, *BSc(ITEng), MSc(InfoSec)*
Doctoral Candidate, School of Computer Science and Software Engineering
University of Wollongong
Wollongong NSW 2522
AUSTRALIA
Tel: +61 2 4221 3074
email: fr683@uowmail.edu.au

Khin Than Win, *MBBS, PhD*
School of Information Systems and Technology
University of Wollongong
Wollongong NSW 2522
AUSTRALIA

Willy Susilo, *BSc(CompEng), MCompSc, PhD*
Professor and Head, School of Computer Science and Software Engineering
University of Wollongong
Wollongong NSW 2522
AUSTRALIA

Appendix

Table 1A: Security and privacy analysis of data collection with ISO 27002:2013 and ISO 29100:2011 standards mapping

PRIVACY AND SECURITY PRINCIPLES	REVIEW ARTICLES	ISO 27002	ISO 29100	SELECTED FEATURES
System and application access control	44[1]	Y[2]	Y	Y
Secure communication	26	Y	Y	Y
Compliance with security requirements	38	Y	Y	Y
Interoperability	17	N[3]	N	Y
Consent & choice mechanism	19	N	Y	Y
Policies and regulations	37	N	Y	Y
Flexibility	16	N	N	Y
Applicability and scalability	22	Y	Y	Y
Integration and sharing	40	Y	N	Y
Cryptography	50	Y	Y	Y
Business continuity	25	Y	Y	Y
Accuracy and quality	20	Y	Y	Y
Operations security	21	Y	Y	Y
Certificates	11	Y	N	N
Data breach notification	1	Y	Y	N
Security checks and updates	1	Y	Y	N
Fault tolerance	2	N	N	N
Maintenance and retrieval service	9	Y	N	N

1 This show 44 of review articles includes 'system and application access control' principle in their design.

2 YES = MENTIONED (standard contains this principle)

3 NO = NOT MENTIONED (standard does not contain this principle)

Table 2A: PRISMA Checklist

TITLE		
Title	1	A systematic literature review on Security and Privacy in …
ABSTRACT		
Structured summary	2	Summary is presented with objective, methods, results, conclusions and key findings
INTRODUCTION		
Rationale	3	The rationale for performing this review was the lack of a coordinated template among EHR systems to provide security and privacy from a technical perspective.
Objectives	4	The objective is to investigate adopted technical EHR security and privacy features …
METHODS		
Protocol and registration	5	The review protocol of our study has been published …
Eligibility criteria	6	Our inclusion criteria were articles published in English which dealt with the security and privacy of the technical implementation …
Information sources	7	The search protocol was applied to Scopus and PubMed digital libraries between 1998 and December 2013.
Search	8	Search strategy is explained in flow chart
Study selection	9	The study search process is based on an advanced search in the Scopus database with defined search keywords, …
Data collection process and data items	10-11	We collected the following data from each article: 1) the author or…
Risk of bias in individual studies	12	The study is done and evaluated by three authors with no bias
Synthesis of results	14	The synthesis is done by cross-case analysis and comparing with ISO standards in NVIVO
RESULTS		
Study selection	17	A flow diagram is presented of studies screened, assessed for eligibility, and included in the review, with reasons for exclusions.
Study characteristics	18	For each study, we presented security and privacy implementations
Results of individual studies	20	Results for each study: simple summary data for each study and intervention groups (users , healthcare providers, etc)
Synthesis of results	21	Presented results of each feature analysis from review studies
DISCUSSION		
Summary of evidence	24	Summarized the main findings
Limitations	25	Study limitations are mentioned as review protocol.
Conclusions	26	Provide a general interpretation of the results and implications for future research.

HEALTH INFORMATION MANAGEMENT JOURNAL Vol 44 No 3 2015 ISSN 1833-3583 (PRINT) ISSN 1833-3575 (ONLINE)
http://dx.doi.org/10.12826/18333575.2015.0001.Rezaeibagha

Table 3A: Systematic literature review results based on the security and privacy implementation in EHR systems

Author	Year	System and Application Access Control	Secure communi-cation	Compliance with standards and regulations	Inter-operability	Consent and Choice	Policies and Regulations	Flexibility	Applicability and Scalability	Integration and Sharing	Crypto-graphy	Business continuity	Accuracy and quality	Operations security
Bernhard Riedl and Veronika Grascher	2010	Authorisation	N[1]	N	N	Integrity attributes, anonymisation	N	N	N	N	Y[2]	N	Quality	Backup
Rui Zhang and Ling Liu	2010	RBAC[3], ABAC[4], Authorisation	SSL/TLS	HIPAA	Common storage format and standards	HIPAA, Cryptographic Access Control	HIPAA, AC[5] policies	N	N	Cloud computing	Y	Availability and Utility-consistency	Accuracy and quality	Backup, audit, archiving
Rui Zhang et al..	2011	Role Based and Time Bound Access Control (RBTBAC)	N	N	N	N	AC policies	Role-based and time-bound access control model (RBTBAC)	Role-based and time-bound access to EHR data	N	Y	Consistency	N	N
Ilaria Matteucci et al.	2011	Authorisation	N	N	N	N	Authorisation, Obligation, Sharing, Management policies	N	N	Set policies to information sharing, EPR	Y	Consistency	N	N
Muhammad Afzal et al.	2011	Authorisation, authentication with Oauth	Standards	HL7	Common storage format and standards, uniform encryption, parallel securing HIE,HL7	N	Nationwide Health Information Network (NHIN) policies	N	Scalable HIE framework	HIE[6]	Y	N	N	N
Ming Li et al.	2013	Fine-grained and scalable data access control	Standards	N	N	N	Access policies	Data access policies should be flexible	ABE[7], MA[8]-ABE, key management, Health cloud	PHR sharing with patient centric platform	Y	Utility and consistency	N	N
Jie Huang et al.	2012	RBAC, DAC	N	N	N	N	AC policies	Flexible access	ABE, Scalable access in multi-cloud	EHR data sharing	Y	N	Quality	N
George Hsieh and Rong-Jaye Chen	2012	RBAC, ABAC, Authorisation	N	HL7	Continuity of Care Document (CCD) standard	N	AC policies, XACML policies	Hierarchical structure	N	Integrated, embedded, and fine- grained cloud-based PHR	Y	N	N	N
Ruoyu Wu et al.	2012	Broker-based access control, Authorisation	N	ISO EHR standard	Policy Manager sub-module, Cloud,	N	AC policies	Access control flexible security mechanism	Applicability	EHR sharing in Cloud	Y	N	N	N
Subrata Acharya et al.	2013	N	Firewall, VPN[9], network segregation ,SSL/TLS	HIPAA	N	N	Security policies, HIPAA regulations	Unparalleled flexibility	N	Secure EHR exchange for sharing	Y	N	Accuracy and quality	Monitoring and logging
Linke Guo et al.	2012	Authentication	SSL/TLS	N	N	N	Privacy policies	N	N	PHR	N	N	N	N
M. Fahim Ferdous Khan and Ken Sakamura	2012	RBAC-A	Encryption, authentication, hybrid AC	HL7, HIPAA	N	DAC[10], RBAC, HIPAA	Fine-grained, flexible and context-based access control policies and statutory regulations	Fine-grained, flexible and context-based access control policies	HL7	N	Y	N	N	N
Chien-Hsing Wu et al.	2013	DAC, MAC[11], RBAC, Authorisation	N	N	N	N	Security policy	N	N	PHR cloud	Y	N	N	N
Anne-KatrinWickboldt and Selwyn Piramuthu	2012	N	N	N	N	N	N	N	N	N	Y	N	N	N
Chia-Hui Liu et al.	2012	Authorisation	Firewall, VPN	HIPAA	N	N	Medical regulations	Flexible security implementation	Applicability	N	Y	Availability	Quality	Archiving
Chanying Huang et al.	2012	N	N	N	N	N	N	Flexible configuration of encryption	Applicability and Scalability of rules	N	Y	N	N	Monitoring and logging
Tsung-Chih Hsiao et al.	2012	N	N	HL7	N	N	Regulations	N	HL7 based on SOA	Integrated Medical Information System	Y	N	Accuracy	N

Table 3A: Systematic literature review results based on the security and privacy implementation in EHR systems continued

Author	Year	System and Application Access Control	Secure communi-cation	Compliance with standards and regulations	Inter-operability	Consent and Choice	Policies and Regulations	Flexibility	Applicability and Scalability	Integration and Sharing	Crypto-graphy	Business continuity	Accuracy and quality	Operations security
Yu-Yi Chen et al.	2012	Access control, authorisation	N	HIPAA	N	ACL[12], digital rights management (DRM) technology	HIPAA policy	N	N	EHR sharing and integration system in healthcare clouds	Y	Availability and Utility	Accuracy	Audit and archiving
Tzer-Shyong Chen et al.	2012	Dynamic access control, Authorisation	N	HL7, HIPAA	N	N	Dynamic access policies	Multi-user dynamic access control	HL7, Health cloud	PHR in cloud	Y	Availability and consistency	Quality	N
Tian-Fu Lee et al.	2013	N	N	N	N	N	N	N	N	Integrated EPR Information System	Y	N	N	N
Asma AlJarullah and Samir El-Masri	2013	Authorisation	VPN	HL7	Health Information System Broker (HISB)	Explicit consent before data extraction	Security policies	3- tier architecture	Semi-centralised architecture Health cloud	National Integration of EHRs	Y	Availability and accessibility-Continuity of Care and consistency	Quality	Audits
Marc Stauch et al.	2013	Access control	N	N	N	Explicit consent before data extraction	Hospital data governance policies	N	Applicability and scalability, PONTE platform	Integrated platform	Y	N	N	N
Gregor von Laszewski et al.	2011	RBAC, Authorisation	SSL/TLS	N	Security Assertion Markup Language (SAML) , IHE	N	N	N	N	eMOLST project, EHR sharing	Y	N	Accuracy and quality	Audits
Charles Safran and Howard Goldberg	2000	Access control	SSL/TLS	HIPAA	N	N	Security policy	N	N	N	Y	N	N	N
Berndx Blobel	2000	Access control and Authorisation	N	Standard	CEN prENV 13606, Part 3 policy	N	Policies	N	Applicability and scalability	N	Y	Consistency	N	N
Bernd Blobel and Francis Roger-France	2001	Access control and Authorisation	VPN, SSL/TLS, standards	HL7	Common policies	Explicit written consent signed	Policies and regulations	N	N	N	Y	Availability	N	Audit trails
M. van der Haak et al.	2003	RBAC	Firewall, VPN	HL7	N	Explicit written consent signed	Legal regulations	N	N	Cross-institutional EPR	Y	Availability	Quality	N
Bernd Blobel	2004	RBAC	Standards	HL7	N	Informed consent	Authorisation, Obligation, Refrain, Delegation, Composite policies	N	Enterprise Security Integration Scalable Framework	Shared care information system	Y	N	N	N
Bernd Blobel, Peter Pharow	2007	Access control and Authorisation	Standards	HL7	Formal computation independent models (CIM)	N	N	Component-orientation for	Component-orientation	Shared care information system	Y	Availability	Quality	N
Thomas Neubauer and Johannes Heurixb	2011	Authorisation	Encryption, anonymisation	HL7,HIPAA	N	N	N	N	N	N	Y	Availability	Quality	N
Barry Barber	1998	N	Standards	Standard	N	Explicit consent before data extraction	Regulations	N	N	N	Y	Availability	N	N
Dixie B. Baker and Daniel R. Masys	1999	RBAC	SSL/TLS	HL7	N	N	RBAC policy, security policy	N	N	PCASSO	Y	N	N	Audits
Omar Bouhaddou et al	2012	RBAC	N	HL7	Standards and Interoperability (SandI) Program	ACL(Access Control List)	Information sharing policies	N	Applicability of standards	N	Y	Continuity	Quality	N
Sergio Martínez et al.	2013	N	N	HIPAA	N	N	N	N	N	N	Y	Utility	N	N
Bernd Blobel and Peter Pharow	2006	RBAC	Standards	HL7	Agreed vocabularies	N	Security policies	Security policies, multi model	N	N	N	N	N	N

HEALTH INFORMATION MANAGEMENT JOURNAL Vol 44 No 3 2015 ISSN 1833-3583 (PRINT) ISSN 1833-3575 (ONLINE)
http://dx.doi.org/10.12826/18333575.2015.0001.Rezaeibagha

Table 3A: Systematic literature review results based on the security and privacy implementation in EHR systems continued

Author	Year	System and Application Access Control	Secure communi-cation	Compliance with standards and regulations	Inter-operability	Consent and Choice	Policies and Regulations	Flexibility	Applicability and Scalability	Integration and Sharing	Crypto-graphy	Business continuity	Accuracy and quality	Operations security
Flora S. Tsai	2010	Access Control	Firewalls, standards	HL7,HIPAA	Cross-enterprise document sharing (XDS)	Explicit consent	Privacy policies	N	N	N	Y	Availability and continuity	N	N
Tony SAHAMA and Evonne MILLER	2011	Access Control	Data encryption	N	N	N	N	N	N	Information sharing	Y	N	Accuracy	Monitoring
Kostas PANTAZOS et al.	2011	N	N	N	N	N	N	N	N	N	Y	consistency	Accuracy	N
S Toh et al.	2011	RBAC	N	N	Flexible network architecture	N	Privacy , governance policies	N	Scalable network architecture	N	Y	Consistency	Accuracy	Monitoring and Audit
Tracey L. Murray et al.	2011	Authorisation	Standards	HL7,HIPAA	N	ACL	HIPAA, governing, confidentiality ,HITECH policies	N	N	N	Y	N	N	N
Jing-song Li et al.	2011	Access control	VPN,SSL/TLS, standards	HL7	Encapsulation, SOA	N	N	Three-level configuration	N	HIE	Y	Consistency and continuity	N	Backup
Shawn N Murphy et al.	2011	Authorisation	N	HIPAA	N	Explicit consent before data extraction	Security policies, HIPAA regulations	N	N	N	Y	Consistency	N	Backup and monitoring
V. BALDAS et al.	2010	RBAC	N	N	N	N	AC policies	N	N	N	Y	N	N	N
teremine Tharaud et al.	2010	Authentication	N	Agreed obligations	N	N	Privacy policies	N	N	N	Y	N	N	N
Christian Stingl and Daniel Slamanig	2011	Access control, Authorisation	SSL/TLS, encryption, anonymization	Standard	N	N	Security policies	N	Health cloud	N	Y	Availability	Quality	Backup
Jinyuan Sun et al.	2011	Access control, Authorisation	encryption, anonymization	HIPAA	N	Explicit consent before data extraction	HIPAA regulations	N	N	N	Y	Availability and Consistency	N	Backup and monitoring
Ramkinker Singh et al.	2013	Access control, Authorisation	N	Standard	N	N	Access policies	Attribute-based access control (ABAC), CC MA-ABE	Health cloud	PHR Sharing in a Patient centric Model in Cloud PHR sharing centric Model in Cloud	Y	N	N	Audits and monitoring
J. Santos et al.	2010	N	N	Standard	Interoperable PHR	N	AC policies	N	Portable PHR (pPHR)	N	Y	N	N	Audits and backup
Cândido Santos et al.	2011	N	Standards	HL7	N	Explicit consent	N	N	Personal Health Record (PHR) design	N	Y	N	N	Monitoring s
Benjamin Burton et al.	2013	Access control, Authorisation	N	HIPAA	N	Informed consent	Policies and regulations	N	Applicability and Scalability of rules	N	Y	N	N	Audits
Euzelia S. Hunter	2013	Access Control, Authorisation	N	HIPAA	N	N	Privacy and legal Regulations	N	N	N	N	Consistency and continuity	Quality	N
Johnathan Coleman	2013	N	N	Standard	Standards	N	N	N	N	N	N	N	N	N
Isla S. Mackenzie et al.	2011	Access rights controls	Firewalls, VPN	N	N	Explicit consent	Policies	N	N	N	Y	N	N	Monitoring and backups
Margaret J. Blythe, MD Mark A. Del Beccaro, MD	2012	Access Control, Authorisation	N	HIPAA	N	Explicit consent	Policies	Standards	N	N	Y	Availability	Quality	N
Lara Khansa et al.	2012	Access management	N	Standard	Standardised cloud computing	N	Privacy and security policies, regulations	N	N	N	Y	N	N	N

Notes:
1 No = does not have this feature
2 Yes = has this feature
3 Role-based access control
4 Attribute-based access control
5 Access control
6 Health information exchange
7 Attribute-based encryption
8 Multi-authority
9 Virtual private network
10 Discretionary access control
11 Mandatory access control
12 Access control list