Multi-authority security framework for scalable EHR systems

Rezaeibagha, F.; Mu, Y.; Susilo, W.; et.al.

Rezaeibagha, F., Mu, Y., Susilo, W., & Win, K. T. (2016). Multi-authority security framework for scalable EHR systems. International Journal of Medical Engineering and Informatics, 8(4), 390–408.
https://doi.org/10.1504/IJMEI.2016.079368
Document Version: Published (Version of Record)

Published Version: https://doi.org/10.1504/IJMEI.2016.079368

Multi-authority security framework for scalable EHR systems

Fatemeh Rezaeibagha*, Yi Mu and Willy Susilo

Centre for Computer and Information Security Research,
School of Computing and Information Technology,
University of Wollongong,
NSW, Australia
Email: fr683@uowmail.edu.au
Email: ymu@uow.edu.au
Email: wsusilo@uow.edu.au
*Corresponding author

Khin Than Win

School of Computing and Information Technology,
University of Wollongong,
NSW, Australia
Email: win@uow.edu.au

Abstract: Electronic health record (EHR) systems can be operated in a large-scale distributed environment, such as cloud computing, which might have to be managed by multiple authorities who control the access to patient records. In this way, a large amount of data from patients can be hosted on a large-scale distributed system. Unfortunately, the security of such systems is usually inadequate, which results in the hindrance of the EHR systems adoption in practice. Attribute-based systems have been a popular choice that could provide a flexible and reliable access control to EHR databases, which are usually managed by a single authority, who is responsible for setting up the system's policy. In a large-scale distributed system, it might be necessary to have multiple authorities, who can handle users located in different areas. Nevertheless, one of the challenges is how to enable multiple authorities with a single access policy. In this paper, we provide a sound solution to this issue. Our EHR system provides a secure environment for EHR users to use the system conveniently and provide the flexibility and scalability.

Keywords: electronic health record; EHR; security; privacy; access control; encryption.

Reference to this paper should be made as follows: Rezaeibagha, F., Mu, Y., Susilo, W. and Win, K.T. (2016) 'Multi-authority security framework for scalable EHR systems', *Int. J. Medical Engineering and Informatics*, Vol. 8, No. 4, pp.390–408.

Biographical notes: Fatemeh Rezaeibagha received his BS of IT Engineering from Islamic Azad University, Iran, and MS of Information Security from Lulea University of Technology, Sweden, in 2010 and 2013, respectively. She is currently pursuing her PhD degree with the School of Computer Science and Software Engineering, University of Wollongong, Australia. Her major research interests include data security, privacy and cryptography in electronic healthcare systems.

Yi Mu received his PhD from Australian National University, in 1994. He is currently Professor, Head of the School of Computer Science and Software Engineering, and co-Director of the Centre for Computer and Information Security Research with the University of Wollongong, Australia. His current research interests include information security and cryptography. He is the Editor-in-Chief of the *International Journal of Applied Cryptography*, and serves as an Associate Editor for ten other international journals. He is a member of the International Association for Cryptologic Research.

1 Introduction

The Electronic Health Record Committee in the Health Information Management Systems Society (HIMSS) defined electronic health record (EHR) using this statement: "The electronic health record (EHR) is a secure, real-time, point-of-care, patient-centric information resource for clinicians. The EHR aids clinicians' decision making by providing access to patient health record information where and when they need it by incorporating evidence-based decision support" (Davis and LaCour, 2014). The 2003 ISO/TS 18308 references the IOM 1991 definition and CEN 13606 2000 to define an EHR system as "a system for recording, retrieving and manipulating information in electronic health records" (Dickinson et al., 2004).

EHR has numerous advantages for improving the quality of diagnosis and reducing the medical costs and errors in order to address reliable and efficient healthcare processes. The exchange of health information is a crucial component to enable provision of high-quality health services. Meanwhile, one of the key issues in electronic healthcare is to share patient records across enterprises. Healthcare providers are required to share and distribute EHR data among necessarily interested parties to provide access to healthcare resources and achieve EHR advantages.

Deploying cloud services in the health sector can facilitate the exchange of medical data among entities and act as the medical record storage but require some certain level of protections (Abbas and Samee, 2014). In this regard, several regulations and standards such as HITECH Act, HIPAA, HL7 CDA, CEN 13606 EHRcom and openEHR proposed guidelines and frameworks for sharing and exchanging health information via the digital representation of clinical data between different entities across healthcare communities. In the following section, we outline some Health IT standards proposed for healthcare data exchange and data sharing.

1.1 Health IT standards

Health Level-7 (HL7) is an acceptable messaging standard that refers to a set of flexible international standards, guidelines and methodologies for clinical and administrative data exchange among software applications used by various healthcare providers. These standards can ensure healthcare system interoperability and EHR sharing or integration through a set of rules in a consistent process (HL7, n.d.). The HL7 EHR system Functional model provides a reference list of functions described from the user perspective, which may be present in an EHR System (EHR-s) to illustrate the granular aspects of functions. The function list designed to enable consistent system functionality (Dickinson et al., 2004; Muñoz et al., 2011; Spooner, 2007).

The personally controlled EHR (PCEHR) in Australia has adopted solutions to establish an IT infrastructure for sharing health information. NEHTA applied this to GP vendor systems implemented a standard profile to deliver a PCEHR system across different locations with the application of IHEXDS (Australia, 2012; Nehta, n.d.). The architecture may include several distributed document repositories that enable the document retrieval procedure (Noumeir and Renaud, 2010; Dogac et al., 2007).

In the field of EHR, Cross-Enterprise Document Sharing (XDS) specification, developed by Integrating the Healthcare Enterprise (IHE) addresses the needs for registration, distribution and access to patient clinical information across healthcare enterprises under a document sharing governance structure agreed by all parties involved. It employs structured EHR standards such as Continuity of Care Record (CCR) and Clinical Data Architecture (CDA) to facilitate data exchange. In order to facilitate the application of XDS specification towards the use of ISO 13606, it enables an EHR_Extract to be stored within an XDS repository.

IHE solely sets up the foundation for EHR interoperability amongst care domains within single/multiple healthcare enterprises and addresses privacy and security controls through risk assessment and management. Privacy and security are enabled and enforced at different levels of depth. IHE recognises audit trail specifically centralised structure as the primary method of accountability enforcement in the healthcare environment (Sinha et al., 2012; Ribeiro et al., 2012; Rezaeibagha et al., 2015).

The CEN/ISO 13606 Electronic Health Communication (EHRCOM) (CEN/ISO, n.d.) is a European norm from the European Committee for Standardization (CEN/TC251) being designed to achieve semantic interoperability in the EHR communication. It can be harmonised with IHE XDS, and consequently XDS can store and share 13606 EHR_Extract data. Nonetheless, it specifies neither the internal architecture of an EHR system nor the way that data is stored (Maldonado et al., 2012). HL7 can be considered to be the foundation of integrated healthcare environments with CEN/ISO 13606 standard (Begoyan, 2007).

The ISO 22600: 2014 standard 22600-1 (2014) “defines principles and specifies the services needed for managing privileges and access control” to data and functions. The ISO 22600-1 is intended to support their technical implementation and also proposes a template with XML for the policy agreement. The policy ideally should be harmonised and security standards defined by CEN and ISO ought to be the primary tools for achieving this. It uses cryptography to support digital signatures over a set of assigned attributes. There is a policy ID attribute as references to policies in granularity level and system hierarchy. As stated, any attribute authority (AA) can be defined, however, it has not specified the implementation.

Although several health IT standards have mandated for data sharing, there are still non-standardised communication architectures and models, which have caused semantic divergences. Since healthcare environment is a broad domain with different sub-domains and a huge number of users, it needs to provide security, interoperability, and scalability to share and access EHR data. Accordingly, healthcare providers are responsible for protecting their data to ensure proper access controls are in place. In this paper, we explore existing studies and introduce a security framework, where the EHR system is managed by multiple authorities, along with a set of protocols for the implementation of the framework. In accordance with the recent development of data sharing, we notice that attribute-based encryption (ABE) can be well fitted into our scenario thanks to its excellent structure that suits well to our framework.

The notion of ABE was introduced by Sahai and Waters (2005) as a solution to enable fine-grained access control for encrypted data. The beauty of ABE is that the fine-grained access control is achieved through some cryptographic techniques rather than traditional access control mechanisms. Pirretti et al. (2010) demonstrated that ABE system is an efficient solution for securely managing data in large distributed and loosely-coupled systems with the HIPAA compliant distributed file system. Moreover, ciphertext-policy attribute-based encryption (CP-ABE) was proposed by Bethencourt et al. (2007) to provide complex access control with encrypted data and keep data confidential even if the storage server is untrusted. This is achieved by embedding the policy in the ciphertexts directly. The main drawback of the ABE system is the basic requirement that needs to have a central authority. Subsequently, Lewko and Waters (2011) addressed this issue by proposing a decentralised ABE, which allows multiple authorities to share the same set of attribute policies. This work has enabled new emerging applications to the large-scale distributed systems, such as cloud computing.

In this work, we enhance this direction of research by proposing a secure and privacy preserved EHR system framework to control the access to EHR data. To illustrate our idea, we incorporate Lewko and Waters' (2011) scheme in our proposed framework to enable such a system. Specifically, we adopt the multi-authority system to our framework to guarantee its practicality. Our EHR system ensures security and scalability features in a distributed environment such as cloud computing. We present the details of EHR data access control using attribute-based cryptography and concerning the secure communication channel between EHR system users and multiple authorities.

1.2 Related work

In the following, we present a review of related work on security and privacy in EHR systems. To start, we highlight the following properties that have been proposed in some of the review studies as follows.

- *Flexibility:* The data access policies and access structure should be flexible to provide efficient EHR data access, especially in emergencies.
- *Scalability:* The EHR system should be scalable to provide accessibility for users from public domain/cloud other than the private domain/cloud. The EHR system scalability could be in terms of key management, storage, access structure, computation, and communication.

- *Confidentiality:* Unauthorised users should be prevented from accessing or decrypting EHR data by proper security implementation, including access control and cryptographic techniques.
- *Sharing:* The EHR system model should be designed in a way that can share any part of EHR with proper authorisation.

Bond et al. (2013) proposed an electronic transfer of prescription (ETP) based on National eHealth Transition Authority (NEHTA) with Unified Markup Language (UML). The framework is based on using RM-ODP standards to provide guidelines and support e-Health systems at Australia's national level. Their ETP system architecture was proposed for the public key infrastructure (PKI) model with credentialing and enrolment functions. Moreover, their interoperable framework facilitates information sharing and NEHTA outcomes' consistency.

Alshehri et al. (2012) proposed a cloud-based EHR system, which consists of the cloud-based data storage and computing resources, health providers (users), and attribute authority (AA). In this work, one single AA is responsible for key management, including generation, distribution, and revocation in the EHR system. They considered a CP-ABE scheme and organised EHR to the labelled hierarchical data structure to provide flexibility, scalability, and fine-grained access control.

In Wu et al. (2013), private key generator (PKG) service for key generation computes the private key of the user that is being used to recover encrypted key for encrypting/decrypting the PHR dataset. EHR trusted server serves as the root PKG for encrypting EHRs and generating private/decryption keys for EHR owners, domain servers, and entities.

Barua et al. (2011) in ESPAC framework (patient-centric access control scheme for e-health in cloud) designed an access control structure that e-healthcare provider works as a trusted party to perform the registration process to generate the keys and trusted authority assigns a unique ID to the healthcare provider. Zhang et al. (2011) proposed an EHR security model with role-based and time-based access control model (RBTBAC) with one trusted authority (TA) to provide flexibility. TA contains two parts for encrypting EHR data and enforcing predefined access control policies.

Some studies have aimed to implement cryptographic techniques such as ABE schemes to provide security and privacy of EHR data. Xhafa et al. (2015) designed a secure cloud-based EHR system with ABE for efficiently storing and sharing PHRs where they applied global authority in the EHR system, responsible for the key management. In another study, Xhafa et al. (2014) proposed a PHR service system to provide the efficient searching, fine-grained access control, and PHR data sharing with anonymous ABE in the hybrid cloud environment.

Liang et al. (2012) proposed attribute-oriented authentication and transmission schemes for secure and privacy-preserving health information sharing in health social networks (HSNs). Huang et al. (2012) proposed an EHR data sharing framework that combines identity-based encryption (IBE) and ABE to enforce access control policies and scalable access between different clouds.

Li et al. (2013) presented an ABE-based patient-centric, secure and scalable PHR sharing framework with the security mechanisms for cloud-based PHRs in the semi-trusted servers. They applied a combination of Chase and Chow (2009) and Yu et al. (2010) MA-ABE schemes from KP-ABE in which data owners are TA of their data to manage the keys and access rights. Yu et al. (2010) proposed the secure, scalable and

fine-grained data access control in the cloud with KP-ABE, proxy re-encryption, and lazy re-encryption. In this proposed scheme, the data owner can define flexible access structure for system users. Ion et al. (2012) designed an access control with KP-ABE for e-health systems. There is one TA to generate the encryption and decryption keys. This work also follows a single authority implementation to distribute keys to the users.

Yang et al. (2013) designed an attribute-based access control for multi-authority systems in cloud storage, whereas there is a globally trusted certificate authority (CA) to set-up the system, register all the users and AAs, and assign a global user identifier and authority identifier for each authority. A seminal study in this area is the work of Yang and Jia (2012) that proposed scalable data access control for multi-authority cloud storage systems. While they mentioned their scheme does not require any global authority for key management, there is one CA as globally trusted certificate authority. In Wang et al. (2012), PHR CP-ABE platform, one AA administrates the secret keys based on Waters CP-ABE scheme.

Benaloh et al. (2009) presented a patient controlled encryption (PCE) system to enable patients to share their partial access rights with others. They aimed to guarantee efficient access, easy sharing and efficient searching over records. Narayan et al. (2010) proposed a privacy-preserving EHR system with ABE infrastructure to share patients' data among healthcare providers in a flexible and scalable manner. They applied one TA to generate the private key and a public directory to store public values of the system.

In some proposals (Alshehri et al., 2012; Anderson, 2008; Chen et al., 2012), the healthcare provider can outsource EHR data and patients can specify access policies in agreement with the TA or healthcare provider. TA is an abstract entity, which is formed by all EHR authorities. TA is responsible for key distribution and issuing credentials of a patient's PHR. TA is considered as the centre to build the access control structure of communication among system users and EHR systems (Chen et al., 2012). In Zhang et al. (2011), TAs are responsible for EHR data encryption from EHR providers into ciphertext format and access control that enforces predetermined access control policies with a remote EHR database to store the encrypted EHR data.

Although all the studies reviewed so far have attempted to provide security of EHR data, they suffer from the fact that one central TA could lead to a large computation overhead through the system expansion. Moreover, users have different attributes associated with their data that cannot be handled with one single TA in a distributed environment. Notably, when there is one single TA who issues all the secret keys then undoubtedly it has the power to access to all EHR data in the system.

In a follow-up study, Chase (2007) presented the multi-authority scheme that supports different attribute authorities issuing secret keys to the users for the different set of attributes. Chase improved this idea in another work by removing the trusted central authority that could monitor all the users' attributes and issues all the decryption keys to the system users. Chase and Chow (2009) proposed that multi-authority ABE enables realistic deployment of attribute-based access control where different attribute authorities issue different set of attributes. In another study, Lewko and Waters (2011) proposed a decentralised CP-ABE scheme to remove the global coordination of the authorities except the initial setup for common reference parameters and some limitations in access policies of Chase's scheme. Implementation of decentralised CP-ABE can reduce key distribution and attribute management overhead on one single TA of the proposed EHR system models.

Table 1 Properties of the related work and our framework

Schemes	*Flexibility*	*Scalability*	*Confidentiality*	*Sharing*	*Cloud-based*	*Multi/ single TA*
Bond et al. (2013)	√	×	√	√	×	Central TA
Xhafa et al. (2014)	×	×	√	√	√	Single TA
Xhafa et al. (2015)	×	×	√	√	√	A global authority
Alshehri et al. (2012)	√	√	√	×	√	One attribute authority
Barua et al. (2011)	×	×	√	×	√	Single TA
Huang et al. (2012)	×	√	√	√	√	Trusted server
Li et al. (2013)	√	√	√	√	√	Multi-TA with KP-ABE
Yu et al. (2010)	√	√	√	√	√	Single TA
Ion et al. (2012)	×	√	√	×	×	Single TA
Yang et al. (2013)	×	×	×	×	√	Single trusted CA
Yang and Jia (2012)	×	√	√	×	√	One CA with MA
Zhang et al. (2011)	√	×	√	×	×	Single TA
Narayan et al. (2010)	√	√	√	√	√	Single TA
Benaloh et al. (2009)	√	×	√	√	×	Single trusted party
Wang et al. (2012)	×	×	√	√	√	Single TA
Liang et al. (2012)	×	×	√	√	×	Single TA
Wu et al. (2013)	×	×	√	×	√	Single TA
Our work	√	√	√	√	√	Multi-authority

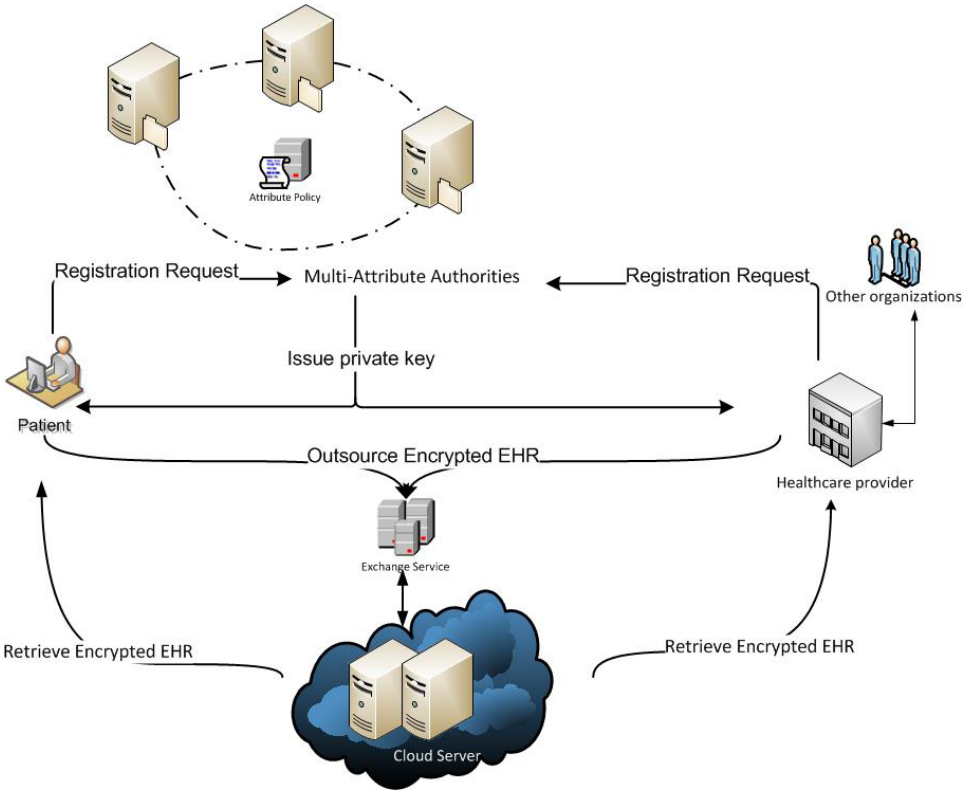
We provide a summary of previous works and our work in Table 1. We believe that our framework moves one step forward by introducing CP-ABE with multi-authority. In comparison to other multi-authority systems, we allow authorities to share the same policy base and issue private keys independently. In Table 1, we present a comparison of our framework and other proposed EHR systems. The merit of our approach is about its feature of distributed management, which prevents 'single points of failure'. That is, if there is a failure in a TA, other TAs can help and make sure the system functions as normal. The accountability can be secured by the separate private key held by TAs. Any action from a TA is associated with its private key, which ensures the responsibility and accountability of the corresponding TA. Again, this feature has been embedded in the original CP-IBE scheme.

2 Model

We design our model by making it be as close to the ETP as possible. As stated in e-Government Strategy by Australian Government Information Management Office

(AGIMO) (2006), in addition to protecting security and privacy as the users' requirements, it is preferred to reform the poorly designed and redundant processes, and reduce the duplication by standardising and combining similar processes across agencies. Moreover, Bond et al. (2013) stated that the ETP system model could be quite complex to demonstrate if the same provider participates in other communities. The ETP architecture can be tailored to the EHR system needs resulting in different solution aspects with different requirements such as security and privacy (Benaloh et al., 2009). The ETP system could be improved in a consistent, flexible, scalable and interoperable framework with our solution.

Figure 1 System model (see online version for colours)



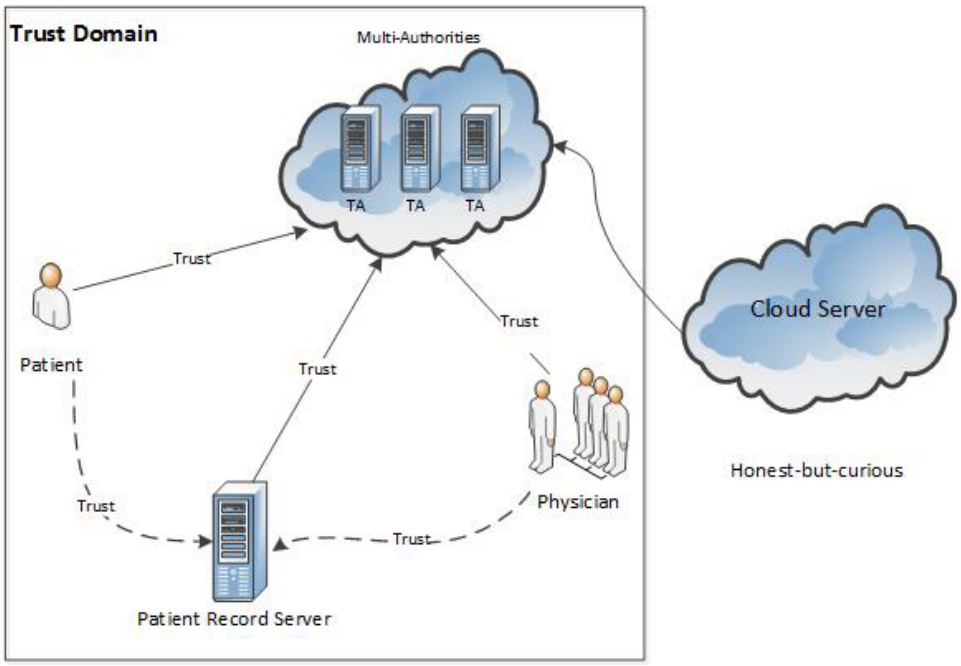
We propose our EHR system model with the decentralised CP-ABE scenario introduced by Lewko and Waters (2011). The model is illustrated in Figure 1. The main design goal of our system is to enable different EHR system users having access to EHR data conveniently in distributed environments such as cloud and enhance privacy and security. The principal users are expected to be authorised healthcare providers, the patient or subject of care who have access to certain functions to their EHR. The healthcare provider receives appropriate decision support to enable effective electronic communication between providers and between the provider and patient or caregiver.

Whereas there is no standard architecture for EHR systems, we provide a basic model for hospital-based EHR system, including the physician, patient, etc. There are different types of data: clinical data, medical and nursing diagnoses, laboratory test results, etc.

The EHR database is located in cloud-storage in encrypted form. The system users outsource and retrieve EHR data from EHR cloud-storage. There are multi-authorities who share an attribute policy base. Patient files are encrypted with proper attributes by any of the authorities. The authorities, who manage the system, can reside in different locations according to the need. A user can access patient records, according to his/her private encryption key, associated with proper attributes.

The ETP is a solution specification developed to facilitate interoperability concerned with transferring electronic clinical documents between prescribers and dispensers. The participants communities in ETP are: subject, prescriber/organisation, dispenser/organisation, prescription exchange service (PES), subject agent, medications supply manager. This architecture includes issuing authority, registration authority, policy authority, and governance authority for credentialing identities in the ETP. The applied identity system is based on the PKI model where enrolment and credentialing are separate functions. On the other hand, as mentioned by Anderson (2008), public key certificates are considered to be 'crypto' rather than 'access control' where their implications for access control policies and architectures are not thought through. In our system, we enable a set of access control policies through different authorities to enable heterogeneous access levels. In this set of policy, we can partition users and resources into domains with distinct administrators, and trust can be inherited between domains (Figure 2).

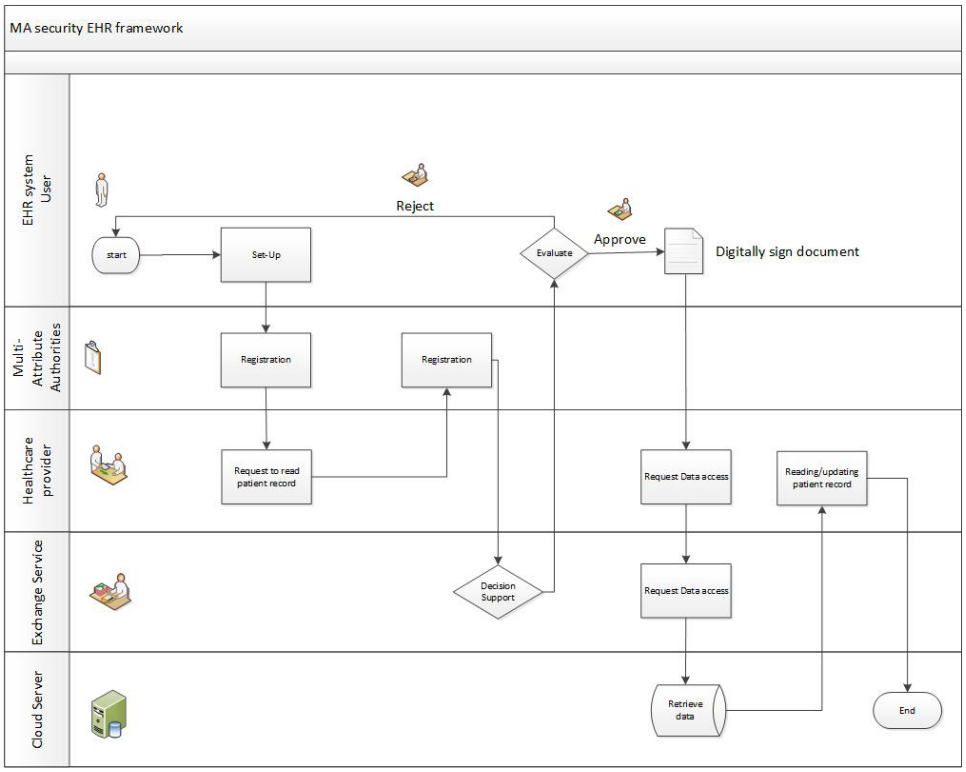
Figure 2 Trust relationship diagram (see online version for colours)



Our system depicts all the participants in a sound comprehensive and generic communication, including healthcare provider (hospital or individual providers) and subject (patient). The individual providers can be doctors and physicians while not any third party, such as supply manager is involved in the system, however, it can be

registered by authorities. The authorities are set-up to perform the enrolment. There are not any credentialing functions owing to replacing certificate authorities by attribute authorities. The access policy is embedded in the attributes that remove the policy authority or any policy management party. We improve privacy by removing the direct access to patient records by the dispenser, supply manager, and prescriber. Any other user than the healthcare provider and patient needs to be registered by multi authorities to gain access to patient data (Figure 3).

Figure 3 Data flow diagram (see online version for colours)



Our model is based on decentralised CP-ABE, which is not based on PKI. Hence, in our system, any need to CA is removed. The benefit of multi-authority is to enable distributed systems and increase the scalability feature by removing the need to CA. Our system is not only an extension of Bond et al.'s work, but it actually provides a much richer access control approach to handling complex EHR systems. Our aim is to provide an alternative approach to handling the EHR systems in distributed systems. Avoiding centralised EHR is one of the goals. Therefore, we should not compare it with Bond et al.'s work directly because our system provides a novel approach for decentralised design. Since it is not based on PKI, our system provides more flexibility to handle access control of EHR. PKI is only applied as part of SSL, which solely provides an authenticated secure channel for data flows (Figure 3). Data flow is explained in details in Section 4.

The trust model can be centralised, distributed or federated. Our system model offers distributed trust model by providing multi-attribute authorities. In accordance with the

centralised model, any single point of failure makes a major bottleneck at the central trust, and consequently the system cannot perform. We resolve this issue with multi-attribute authorities implementation. As shown in Figure 3, there is a peer-to-peer trust relationship in a distributed model. The direct communication, highlighted by arrows, occurs only between trusted parties who are patient, physician, healthcare provider, patient record server, and trusted authorities. The cloud server is an honest-but-curious party and only provides the required data storage (Rezaeibagha and Mu, 2016).

3 Attribute-based security framework with multiple trust authorities

ABE firstly was introduced by Sahai and Waters (2005) where they constructed an IBE of a message under attributes to create a fuzzy identity. There are two forms of ABE presented by Goyal et al. (2006) namely CP-ABE and key-policy attribute-based encryption (KP-ABE). In CP-ABE system, keys are associated with the sets of attributes and ciphertexts are associated with the access policies. Then, the user who has the private key that satisfies the policy can decrypt the ciphertext. In the KP-ABE system, private keys are associated with an access structure and the ciphertext is labelled with a set of attributes. Then, when the access structure defined in the private keys matches the attributes labelled with the ciphertext, a user can decrypt the ciphertext. In our system, policies are controlled by the health authority, such as the hospital as the healthcare provider. Private/public keys are associated with the sets of attributes (CP-ABE). Our system is based on the original security model of CP-ABE, which illuminates all potential attacks aiming to compromise the system. These attacks include collusion attacks, chosen plaintext attacks (or symmetric security), etc. As demonstrated by Bethencourt et al. (2007), CP-ABE is secure against collusion attacks.

Definition 3.1: (trusted authority) Let $T = \{TA_i\}$ for $i = 1,\ldots,n$, a set of n parties, who are fully trusted by all other parties for correctly setting up the system and issuing correct private keys to other parties. They share the same set of policy base that consists of a set of attributes. Any trusted authority $TA_i \in T$ can issue a private decryption key to a user in the system.

Definition 3.2: (access matrix) Let A be an $n \times l$ access matrix and maps its rows to attributes $\{a_i\}$, for $n \times l$, be a set of attributes. Any $a_i \in A$ represents an element used to define the access policy to patient records.

Following the multi-authority CP-ABE system by Lewko and Waters (2011), our proposed EHR system is comprised of the following five algorithms:

- Global-setup. This algorithm takes as input the security parameter k and outputs global parameters GP for the system.
- TA-setup $(GP) \rightarrow SK, PK$. Each TA_i runs the algorithm with GP as input from the global setup phase to produce its own private key (SK) and public key (PK).
- Encrypt $(M, (A, \rho), GP, \{PK\}) \rightarrow CT$. The encryption algorithm takes in a message M, an access matrix (A, ρ), the set of public keys for relevant TAs, and the global parameters. It outputs a ciphertext CT.

- KeyGen (GID, GP, i, SK) $\rightarrow K_i$, G_{ID}. It takes as input a global identity G_{ID} (in our EHR system, it represents a user ID), the global parameters, and an attribute i belonging to some TA, and the private key SK for this TA. It produces a key K_i, G_{ID} for this attribute, identity pair.
- Decrypt (CT, GP, K_i, G_{ID}) $\rightarrow M$. The decryption algorithm takes in the global parameters GP, the ciphertext CT, and a collection of keys corresponding to attribute, identity pairs all with the same fixed identity G_{ID}. It outputs either the message M when the collection of attributes i satisfies the access matrix corresponding to the ciphertext. Otherwise, decryption fails.

4 The protocols

We have assumed that our EHR has a set of trusted authorities T, where TA_i 2 T is an abstract entity, which could be a mix of health authorities and hospitals that control the access control policies in order to provide trusted services. For simplicity, we assume that our EHR system consists of a set of *TAs*, a set of patients who have full access rights to their own records, a set of physicians who have some or all access rights granted by a TA to their patient records.

Definition 4.1: (Patient records) Let R_x be a set of patient records wrt patient x. Any element $r_i \in R_x$ for $i = 1,\ldots,n_p$ is encrypted with ABE using a different or the same $\{PK\}$ depending on the access policy. By $\overline{r_i}$ we denote the encrypted record of r_i. Each record is assigned a number or an ID, such as id_{r_i} for record r_i.

In Table 2, as an example, we assume that all patient records are encrypted with the attributed-based encryption algorithm defined earlier. We assume that each item in a patient record is encrypted with a set of attributes, where they may be different or the same for different records, depending on the access policy. In our scenario, attributes are defined as access rights such as ‘read’, ‘write’, ‘delete’, etc. In light of this, there is no need to know the patient’s records for assigning an access privilege to the user.

Table 2 The format of patient records

Patient information		*Attributes*					*EHR*
Patient ID	*Record ID*	a_1	a_2	a_3	$\cdots$	a_n	$\overline{r_i}$
Alice	id_{r_1}	1	0	1	$\cdots$	1	$\overline{r_1}$
	id_{r_2}	1	0	1	$\cdots$	0	$\overline{r_2}$
	id_{r_3}	0	0	1	$\cdots$	0	$\overline{r_3}$
	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
	$id_{r_{n_p}}$	0	0	1	$\cdots$	1	$\overline{r_{n_p}}$
Bob	id_{r_1}	0	1	0	$\cdots$	0	$\overline{r_1}$
	id_{r_2}	0	1	0	$\cdots$	1	$\overline{r_2}$
	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$

It can be seen from the data in Table 2 that all access privileges are associated with unique patient ID, therefore, they cannot be misused. There are record IDs associated with EHR data for users, which are unique and enable EHR encryption. ID is unique to a patient. The attributes embedded in the access key of a user are associated with the unique ID, which avoids any potential collusion. Every user is registered by a TA who assigns proper attributes to the user. 'Null' in Table 2 represents that patient does not have that specific access right to EHR data. Consequently, the uniqueness of a private key can represent the appropriate access. Accordingly, a user can decrypt the record if his key contains the authorised attributes associated with the correct ID. In Table 3, we provide a summary of participants in our protocols.

Table 3 Access arrangement where patient record server could be TA

Party involved	Access rights
TA's	Grant access rights
Patient	Read his/her own records only
Physician/doctor	Read access and/or append new patient records
Patient record server	Encrypt patient records
Cloud server	Null

In the following, we provide the precise definition of the entities involved in the system.

Definition 4.2: (entities involved)

- *Patient:* A patient P is the full owner of its own patient record and has the full trust to the set of TAs (Figure 3) to correctly manage its record and grant correctly access rights to a physician. Patients have only the 'read' right to their own electronic health records.
- *Physician:* A physician or medical specialist D's access rights to the patient records are granted by a $TA \in T$. With its access rights to some or all records, D can read these records and append new information to these records but cannot delete any patient record (item). Physicians must show that they are 'meaningfully using' certified EHRs by meeting certain objectives.
- *Patient record server:* Let S be a patient record server, who is responsible for managing patient records. S is a trusted server, who manages and updates patient records according to the access policy. As an important task for S, it encrypts patient records with the correct public key (attributes).

Notice that patient record server is not the cloud server, but an authorised server by the health authority. A summary of access arrangement of the involved parties is given in Table 3.

4.1 EHR system setup

The trusted authorities in T bear the full responsibility to set the EHR system up by firstly using global-setup. Upon the completion of global-setup, the global parameters GP that is used to construct the cryptographic keys of TAs by using TA-setup. As a result of TA-setup, each TA_i for $i = 1,\ldots,n$ in T holds a private key SK and a public key PK.

4.2 Registration

In the registration phase, each user needs to communicate with a trusted authority (TA_i) in order to obtain its own private key, which we denote as K_i, and is generated in terms of the attribute-based policy. Since all trusted authorities share a policy base, any trusted authority can issue a legal key to a user. Suppose that in the initiation phase, an SSL channel is established and all communication flows hereafter are protected. Note that SSL only provides a secure channel for communication as a standard system setup and is not managed by TA. We omit this phase in the following protocols.

- *Patient (P) registration:*

  1 $P \rightarrow TA_i$: P, REQ_P

  2 $TA_i \rightarrow P$: K_P.

  Here, REQ_P is a request from P for registration to TA_i and K_P is the private key for P to access its own EHR records. K_P is generated by calling the KeyGen algorithm. The KeyGen algorithm takes ID of P, global parameters G_{ID} from TA_i global-setup, and attributes of TA_i with private key K for TA_i to output K_P of P.

- *Physician/doctor (D) registration*

  1 $D \rightarrow TA_i$: D, REQ_D $(P, id_{r_i}, id_{r_j}, \cdots)$

  2 $TA_i \rightarrow P$: $K_{D,P}$.

  Here, $REQ_D(P, id_{r_i}, id_{r_j}, \cdots)$ is a request from D to obtain private decryption keys for the patient P's record IDs $id_{r_i}, id_{r_j}, \cdots \in R_P$. $K_{D,P}$ is the private key for physician (D) to access health records $id_{r_i}, id_{r_j}, \cdots$. $K_{D,P}$ is generated by calling the KeyGen algorithm. The KeyGen algorithm takes ID of D, global parameters G_{ID} from TA_i global-setup, and attributes of TA_i with private key SK for TA_i to output $K_{D,P}$ of D.

- *Record server (S) registration*

  1 $S \rightarrow TA_i$: S, REQ_S

  2 $TA_i \rightarrow S$: PK.

  S receives PK from TA_i, which includes all required parameters for encryption of patient records from TA_i. S can encrypt a record on request of a physician or a patient, according to the attribute-based policy by the encrypt algorithm.

4.3 Patient record management

- *Patient record (item) creation*

  Creation of a patient record could be done when a patient visits its physician. Optionally, it could be done remotely while the patient consults a physician by a computer network. We assume that the creation of a patient record requires the authorisation of the patient.

  1 $D \rightarrow S$: $E_{PK}(P, r)$

  2 S encrypts and stores it as $(P, id_{r_i}, \{a_i\}, \overline{r_i})$.

D generates a record item r_i for patient P. $\{a_i\} \in A$ is a set of attributes, which have been used for the encryption. The patient records stored in the cloud follow the format given in Table 2. The encryption is performed with the Encrypt algorithm. The encryption algorithm takes r_i, with record's ID id_{r_i}, GP of global-setup, and PK of TA_i, then outputs ciphertext $\overline{r_i}$ and stores as $(P, id_{r_i}, \{a_i\}, \overline{r_i})$ in cloud-storage.

- *Reading patient record*

  We assume that the protocol is executed between a user U (patient or physician) and S.

  1 $U \rightarrow S$: P, id_{r_i}

  2 $S \rightarrow U$: $\overline{r_i}$.

  U, who can be the patient or a physician, requests patient record r_i to S. S found the encrypted record $\overline{r_i}$ according to id_{r_i} provided by U. Upon receiving $\overline{r_i}$, U decrypts it with its private key to P: $K_{U,P}$. The decrypt algorithm takes ciphertext $\overline{r_i}$, GP of global-setup, and private key $K_{U,P}$, then outputs decrypted record of r_i.

- *Inserting (update) to a patient record (item)*

  This protocol is executed between a physician D and S.

  1 $D \rightarrow S$: P, id_{r_i}

  2 $S \rightarrow D$: $\overline{r_i}$

  3 $D \rightarrow S$: $E_{PK}(P, r_i')$

  4 S encrypts and stores it as $(P, id_{r_i'}, \{a_i\}, r_i')$.

  Here, r_i' is the updated record wrt r_i. This operation is actually 'appending', where the original content on the record cannot be deleted. Optionally, S can select to use the original id_{r_i}, i.e. $id_{r_i} = id_{r_i'}$.

In the setup stage, a proper SSL session is required to provide a secure and authenticated channel, which ensures that all later communication flows are encrypted and all users know that their communication partners are genuine. This process can be easily built into the system, as the SSL can be implemented easily. SSL is merely used for securing the communication channel and plays no role in our access control structure. It can be set up when HTTPS is installed as all other web-based systems. Our protocols only address the access control part. TAs do not require handling SSL connections.

The patient records are all encrypted with proper attributes. Consequently, only the authorised parties can access these records. It is assumed that the cloud server is managed health authorities who, along with TAs, are trusted by the patients. The cloud server is not authorised to write and update patient records, even though they are trusted to encrypt patient records as an option mentioned earlier. Once a patient record is updated, it must be re-encrypted with the same set of attributes, according to the policy. Once it is encrypted, the cloud server is unable to decrypt.

Global-setup and TA-setup are two important algorithms that allow the authorities to run the system. This process is again protected with an SSL session if the communication

is required. All late protocols are based on the parameters produced from global-setup and TA-setup.

The patient's keys are issued by TAs while we have assumed that TAs have obtained these private keys. Hence, they can access all patient records. Nevertheless, this is a necessary assumption in order to run the system.

5 An application scenario

All patients who receive the treatment in the healthcare system (clinic, hospital, laboratory, etc.) must be registered. The authorities, who are in charge of the system act as TAs, are located at different locations. To take one example, there is an authority for each town or suburb. We assume that each patient holds a valid health card (smart card) as, which holds some basic information about the patient, including the private cryptographic keys to access its health record stored in the cloud server. Each patient must be registered with one of the authorities, who issues all information required to use the healthcare system. This information includes patient name, address, gender, cryptographic keys, etc. Therefore, patients based on their associated attributes can decrypt their data with their own private key (smart card).

In the registration process, patients are given a unique ID (such as social security number or tax number) and password by a local TA to request for a private key from TA which grants access to their own EHR records (if it is not empty). With its key, a patient has full access rights and is able to modify some of its records, such as allergies or new medications taking with its own private key, but cannot delete any existing record. Take Alice in Table 2 as an example. Her cryptographic key should include the attributes for all her health records of $(id_{r_1},\ldots,id_{r_{np}})$.

Medical staff should be registered and authorised health card (a smart card) is issued to each staff. The smart card contains all his/her patients access keys that can be granted by the registration and updated in the future while a new patient is included and an old patient has left.

A physician should be able to access his/her patients' records based on defined access policies and with the private key from a TA, read and update the patients' records in the cloud server. Again, no one can delete any record in the system.

If a patient visits a physician in a clinic due to a splinter in the thumb, to access the patient history (leg, splinter, etc.), firstly, if not yet registered, the physician should register in an online TA to get its own private key. Physician thereupon can decrypt patient data and access the patient's medical records from the server, such as vaccination, principal diagnosis, insurance, identity, etc. If the finger appears to be infected then the physician needs to assign a blood test or extended reviews. The authorised key of the physician should be able to access the future records of the patient.

Taking Table 2 as an example, Alice's physician, Mike holds a key that contains the attributes to access (id_{r_2}, id_{r_3}); therefore, he can access (r_2, r_3) only, but no other records. Mike should hold a table, which contains all his patients' access information. An example is given in Table 4, which shows that he can access Alice's EHR (r_2, r_3) with key $ak_{r_2 r_3}$ and Bob's EHR r_2 with key bk_{r_2}.

Table 4 The access table for Mike

Patient information		*Attributes*					*EHR*
Patient ID	*Record ID*	a_1	a_2	a_3	⋯	a_n	$\overline{r_i}$
Alice	id_{r_2}	1	0	1	⋯	0	$ak_{r_2 r_3}$
	id_{r_3}	0	0	1	⋯	0	
Bob	id_{r_2}	0	1	0	⋯	1	bk_{r_2}

6 Conclusions

We have proposed and described an EHR system model that can provide scalability, and flexibility of EHR systems in distributed environments while preserving privacy and security of EHR data. We investigated one of the solutions to the security and privacy issues on distributed EHR systems, which avoids using a single trusted authority. With ABE, we can provide fine-grained access control and flexible policies for secure EHR system infrastructures. We plan to develop our EHR system model in more details and with the exchange platforms such as HL7. Although our proposed system meets our design requirements, it is worth noting some potential issues about the proposed system. Like all systems, which require security protection, the potential computational cost should be considered for future implementation. We assume that TAs and *S* have powerful computers, which can handle the additional computation overheads owing to the computation of encryption. Consequently, we proposed that TAs and *S* carry out most of the computations while users only require decrypting the corresponding patient's records. This kind of computation can be easily conducted on a normal PC or even a smartphone. The other issue we should consider is the coordination in implementation. By virtue of the nature of distributed systems, the policy updates should be managed by the authorised party. We assume that any *S* can act as the authorised coordinator for the key management.

References

Abbas, A. and Samee, U.K. (2014) 'A review on the state-of-the-art privacy preserving approaches in e-health clouds', *IEEE Journal of Biomedical and Health Informatics*, Vol. 18, No. 4, pp.1431--1441.

Alshehri, S., Radziszowski, S.P. and Raj, R.K. (2012) 'Secure access for healthcare data in the cloud using ciphertext-policy attribute-based encryption', *ICDE Workshops*, pp.143–146.

Anderson, R. (2008) *Security Engineering*, John Wiley & Sons, UK.

Australia, I.H.E. (2012) *Personally Controlled. EHR eHealth Site Grants – Where to from Here?* [online] http://ihe-australia.wikispaces.com/file/view/site+grant+flyer.pdf (accessed 18 May 2015).

Australian Government Information Management Office (AGIMO) (2006) *2006 E-government Strategy, Responsive Government: A New Service Agenda*. [online] http://www.finance.gov.au/publications/2006-e-government-strategy/.

Barua, M., Liang, X., Lu, R. and Shen, X. (2011) 'Espac: enabling security and patient-centric access control for ehealth in cloud computing', *IJSN*, Vol. 6, Nos. 2/3, pp.67–76.

Begoyan, A. (2007) *An Overview of Interoperability Standards for Electronic Health Records*, Society for Design and Process Science, USA.

Benaloh, J., Chase, M., Horvitz, E. and Lauter, K. (2009) 'Patient controlled encryption: ensuring privacy of electronic medical records', *CCSW*, pp.103–114.

Bethencourt, J., Sahai, A. and Waters, B. (2007) 'Ciphertext-policy attribute-based encryption', *IEEE Symposium on Security and Privacy*, pp.321–334.

Bond, A., Hacking, A., Milosevic, Z. and Zander, A. (2013) 'Specifying and building interoperable ehealth systems: ODP benefits and lessons learned', *Computer Standards & Interfaces*, Vol. 35, No. 3, pp.313–328.

CEN/ISO (n.d.) *The CEN/ISO EN13606 Standard* [online] http://www.en13606.org/the-ceniso-en13606-standard (accessed 18 May 2015).

Chase, M. (2007) 'Multi-authority attribute based encryption', *TCC*, pp.515–534.

Chase, M. and Chow, S.S. (2009) 'Improving privacy and security in multi-authority attribute-based encryption', *ACM Conference on Computer and Communications Security*, pp.121–130.

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', *J. Medical Systems*, Vol. 36, No. 6, pp.4005–4020.

Davis, N. and LaCour, M. (2014) *Health Information Technology*, 3rd ed., Elsevier, USA.

Dickinson, G., Fischetti, L. and Heard, S. (2004) 'Hl7 EHR system functional model draft standard for trial use', *Health Level 7*, Citeseer.

Dogac, A., Laleci, G.B., Aden, T. and Eichelberg, M. (2007) 'Enhancing IHE XDS for federated clinical affinity domain support', *IEEE Transactions on Information Technology in Biomedicine*, Vol. 11, No. 2, pp.213–221.

Goyal, V., Pandey, O., Sahai, A. and Waters, B. (2006) *Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data*, 309pp, *Proceedings of the 13th ACM Conference on Computer and Communications Security*, ACM.

HL7 (n.d.) *Health Level 7* [online] http://www.hl7.org.au (accessed 18 May 2015).

Huang, J., Sharaf, M. and Huang, C-T. (2012) 'A hierarchical framework for secure and scalable EHR sharing and access control in multi-cloud', *ICPP Workshops*, pp.279–287.

Ion, M., Russello, G. and Crispo, B. (2012) 'Design and implementation of a confidentiality and access control solution for publish/subscribe systems', *Computer Networks*, Vol. 56, No. 7, pp.2014–2037.

ISO 22600: 2014 standard 22600-1 (2014) *Health Informatics – Privilege Management and Access Control – Part 1: Overview and Policy Management* [online] http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=62653 (accessed 18 May 2015).

Lewko, A. and Waters, B. (2011) 'Decentralizing attribute-based encryption', *Advances in Cryptology – EUROCRYPT 2011*, pp.568–588.

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 Trans. Parallel Distrib. Syst.*, Vol. 24, No. 1, pp.131–143.

Liang, X., Barua, M., Lu, R., Lin, X. and Shen, X.S. (2012) 'Healthshare: achieving secure and privacy-preserving health information sharing through health social networks', *Computer Communications*, Vol. 35, No. 15, pp.1910–1920.

Maldonado, J.A., Costa, C.M., Moner, D., Menárguez-Tortosa, M., Boscá, D., Giménez, J.A.M., Fernández-Breis, J.T. and Robles, M. (2012) 'Using the researcher platform to facilitate the practical application of the EHR standards', *Journal of Biomedical Informatics*, Vol. 45, No. 4, pp.746–762.

Muñoz, P., Trigo, J., Martínez, I., Muñoz, A., Escayola, J. and García, J. (2011), 'The ISO/EN 13606 standard for the interoperable exchange of electronic health records', *Journal of Healthcare Engineering*, Vol. 2, No. 1, pp.1–24.

Narayan, S., Gagné, M. and Safavi-Naini, R. (2010) 'Privacy preserving EHR system using attribute-based infrastructure', *CCSW*, pp.47–52.

Nehta (n.d.) *Shared Health Summary* [online] https://www.nehta.gov.au/implementation-resources/clinical-documents/shared-health-summary (accessed 18 May 2015).

Noumeir, R. and Renaud, B. (2010) 'IHE cross-enterprise document sharing for imaging: interoperability testing software', *Source Code for Biology and Medicine*, Vol. 5, No. 1, p.9.

Pirretti, M., Traynor, P., McDaniel, P. and Waters, B. (2010) 'Secure attribute-based systems', *Journal of Computer Security*, Vol. 18, No. 5, pp.799–837.

Rezaeibagha, F. and Mu, Y. (2016) 'Distributed clinical data sharing via dynamic access-control policy transformation', *International Journal of Medical Informatics*, May, Vol. 89, pp.25–31.

Rezaeibagha, F., Win, K.T. and Susilo, W. (2015) 'A systematic literature review on security and privacy of electronic health record systems: technical perspectives', *Health Information Management Journal*, Vol. 44, No. 3, p.23.

Ribeiro, L.S., Costa, C. and Oliveira, J.L. (2012) 'Enhancing the many-to-many relations across IHE document sharing communities', *Stud Health Technol. Inform.*, Vol. 180, pp.641–645.

Sahai, A. and Waters, B. (2005) 'Fuzzy identity-based encryption', *EUROCRYPT*, pp.457–473.

Sinha, P.K., Sunder, G., Bendale, P., Mantri, M. and Dande, A. (2012) *Electronic Health Record: Standards, Coding Systems, Frameworks, and Infrastructures*, John Wiley & Sons, 27 November.

Spooner, S.A. (2007) 'Special requirements of electronic health record systems in pediatrics', *Pediatrics*, Vol. 119, No. 3, pp.631–637.

Wang, C., Liu, X. and Li, W. (2012) 'Implementing a personal health record cloud platform using ciphertext-policy attribute-based encryption', *INCoS*, pp.8–14.

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*, pp.1–5.

Xhafa, F., Li, J., Zhao, G., Li, J., Chen, X. and S. Wong, D. (2015) 'Designing cloud-based electronic health record system with attribute-based encryption', *Multimedia Tools and Applications*, Vol. 74, No. 10, pp.3441–3458, Springer.

Xhafa, F., Wang, J., Chen, X., Liu, J.K., Li, J. and Krause, P. (2014) 'An efficient PHR service system supporting fuzzy keyword search and fine-grained access control', *Soft Computing*, Vol. 18, No. 9, pp.1795--1802, Springer.

Yang, K. and Jia, X. (2012) 'Attributed-based access control for multi-authority systems in cloud storage', *ICDCS*, pp.536–545.

Yang, K., Jia, X., Ren, K., Zhang, B. and Xie, R. (2013) 'DAC-MACS: effective data access control for multi-authority cloud storage systems', *INFOCOM*, pp.2895–2903.

Yu, S., Wang, C., Ren, K. and Lou, W. (2010) 'Achieving secure, scalable, and fine-grained data access control in cloud computing', *INFOCOM*, pp.534–542.

Zhang, R., Liu, J., Han, Z. and Liu, L. (2011) 'RBTBAC: secure access and management of EHR data', *International Conference on Information Society*, pp.494–499.