1-1-2013

# Secure exchange of electronic health records

Alejandro Flores Zuniga
*University of Wollongong*, aefz871@uow.edu.au

Khin Than Win
*University of Wollongong*, win@uow.edu.au

Willy Susilo
*University of Wollongong*, wsusilo@uow.edu.au

## Recommended Citation

Flores Zuniga, Alejandro; Win, Khin Than; and Susilo, Willy, "Secure exchange of electronic health records" (2013). *Faculty of Engineering and Information Sciences - Papers: Part A*. 2467.
https://ro.uow.edu.au/eispapers/2467

## Secure exchange of electronic health records

### Abstract

Protecting the confidentiality of a patient's information in a shared care environment could become a complex task. Correct identification of users, assigning of access permissions, and resolution of conflict rise as main points of interest in providing solutions for data exchange among health care providers. Traditional approaches such as Mandatory Access Control, Discretionary Access control and Role-Based Access Control policies do not always provide a suitable solution for health care settings, especially for shared care environments. The core of this contribution consists in the description of an approach which uses attribute-based encryption to protect the confidentiality of patients' information during the exchange of electronic health records among healthcare providers. Attribute-based encryption allows the reinforcing of access policies and reduces the risk of unauthorized access to sensitive information; it also provides a set of functionalities which are described using a case study. Attribute-based encryption provides an answer to restrictions presented by traditional approaches and facilitate the reinforcing of existing security policies over the transmitted data.

### Keywords

health, exchange, secure, records, electronic

### Disciplines

Engineering | Science and Technology Studies

### Publication Details

Flores Zuniga, A., Win, K. & Susilo, W. (2013). Secure exchange of electronic health records. User-Driven Healthcare: Concepts, Methodologies, Tools, and Applications (pp. 1403-1424). United States: Medical Information Science Reference.

# Secure exchange of Electronic Health records

**Alejandro Enrique Flores, Khin Than Win and Willy Susilo**
*Faculty of Informatics, University of Wollongong, Wollongong, NSW, Australia*

## ABSTRACT

Protecting the confidentiality of a patient's information in a shared care environment could become a complex task. Correct identification of users, assigning of access permissions, and resolution of conflict rise as main points of interest in providing solutions for data exchange among health care providers. Traditional approaches such as Mandatory Access Control, Discretionary Access control and Role-Based Access Control policies do not always provide a suitable solution for health care settings, especially for shared care environments. The core of this contribution consists in the description of an approach which uses attribute-based encryption to protect the confidentiality of patients' information during the exchange of electronic health records among healthcare providers. Attribute-based encryption allows the reinforcing of access policies and reduces the risk of unauthorized access to sensitive information; it also provides a set of functionalities which are described using a case study. Attribute-based encryption provides an answer to restrictions presented by traditional approaches and facilitate the reinforcing of existing security policies over the transmitted data.

## INTRODUCTION

In a shared care paradigm, remote access to distant data repositories along with the exchange of relevant electronic health records (EHRs) becomes essential for providing integral health care services. Internet is the natural platform to support such functionalities. However, the insecure nature of the network and the increased amount of health information transmitted through it raise the concern over the secure exchange of EHRs (Ohno-Machadoa, Silveira, & Vinterbo, 2004). In fact, the disclosure, transmission and use of patient's data for delivering health care services are an expanding practice that concerns the interest of health institutions, physicians and patients. In a dynamic and demanding environment, such as health care, a patient's confidentiality can only be guaranteed by incorporating security services and mechanisms along with common security policies and/or conflict resolution policies to protect the data at any given point(Lopez & Blobel, 2009). Additionally, EHR systems not only should assure the protection of patients' privacy and confidentiality but also guarantee the reliability and integrity of the information gathered by health care professionals (Conrick & Newell, 2006). Therefore, it is essential that health information systems consider the privacy and integrity of the data and also allow the safe retrieval of information for primary and secondary uses, especially in an interconnected health information scenario (Lusignan, Chan, Theadom, & Dhoul, 2007).

In this context, projects centered in the interconnection of health information systems, such as national health information initiatives or multi-domain EHR systems, not only confront information and functional requirements, such as the development and implementation of standardized communication protocols, standardized vocabulary and homogeneous development frameworks, but also privacy and security requirements. Protection of a patient's privacy and the secure disclosure of health information are crucial functionalities that should be embedded within the specifications of modern and reliable electronic health record systems (Conrick & Newell, 2006; Ohno-Machadoa, et al., 2004; Safran, et al., 2007). Moreover, to guarantee the secure transmission and release of health information in a shared care paradigm, the protection of a patient's privacy has to be conceived as an issue which combines the secure transmission of data, correct user authentication, access control and security policies, either at the point of origin or at the destination of the communication channel.

During the exchange of EHRs, even when the transmission has been between trusted parties, access permission can be violated under specific circumstances. Consider a scenario in which health care institutions A and B are trusted parties during the exchange of information. Using public key technologies both institutions can transmit information using a secure channel. The secure channel guarantees confidentiality and integrity of the transmitted information. However, the existence of different access policies may lead to a violation of access permissions either at the point of origin or when the information reaches its destination. Blobel et al. have suggested the definition of common domain policies to address differences or conflicts rising from disparities in the definition of security and access policies existing among health care organizations (Blobel, Nordberg, Davis, & Pharow, 2006). However, implementing this approach requires the existence of standardized vocabularies and common policy structures, which is limited in the actual health information infrastructure. There is also a virtual agreement that for communication of medical information and posterior access to the data, access policies based on role-based access control models may facilitate the overcoming of possible violation of access permission (Blobel, et al., 2006; Gritzalis & Lambrinoudakis, 2004). However, role-based access control models also present issues that may increase the risk of unauthorized access to sensitive medical data (Alhaqbani & Fidge, 2008).

This chapter aims to address the issues of secure transmission of data, access control and user privileges and propose a specification for an information exchange model that allows a secure and safe approach for the exchange and release of EHR in a shared care scenario. Assuming that transmission of medical information is maintained over insecure channels, we propose a policy reinforcement model based on attribute-based encryptions and incorporate security mechanisms in order to protect patients' privacy during the exchange and release of the information.

## BACKGROUND

Electronic health record should not only be considered as a replacement for paper-based medical records but also means to facilitate the quicker/easier access to relevant health information. EHRs also facilitate the implementation of information architectures to provide support to shared care environments, where communication between the staff involved in imparting care to a patient as well as remote access to data repositories are essential activities. In general, the historical information maintained within the health repositories can also be used as a supporting and knowledge base for continuing treatment of the patient, a base of information for further treatment of the same patient, and base-knowledge for advanced research and medical education.

## Security and privacy of patients' EHRs

The nature of a medical record can be described as information provided by a uniquely vulnerable human being, worried in some manner about the core of his/her very existence, to a trusted person with superior knowledge (Eddy, 2000). In fact, modern electronic health records contain extremely personal and sensitive information regarding not only health history but also the dietary habits, sexual orientation, sexual activities, employment status, income, eligibility for public assistance and family history of a patient (Choi, Capitan, Krause, & Streeper, 2006). Therefore, sharing EHRs raises concerns over the legal and ethical implications associated to the unauthorized access and release of personal information, and the effects that this may cause to the patient (Anderson, 2007; Conrick & Newell, 2006). Patients understand the importance of retaining medical information to support and improve the delivery of health care even when they recognize both the sensitive nature of the collected data and the fact that information contended by computerized health information system becomes more accessible to health professional, administrative and medical staff, and third parties (Conrick & Newell, 2006). Patients expect secure health information systems in which personal data is protected and any disclosed information would be used only for health care purposes (Grain, 2006).

Safe access and exchange of electronic health information requires not only the secure transmission of data but also to ensure that information will be disclosed only to those with the correct access privileges. This implies that protection of patients' privacy needs to be conserved at the source point, when it is transmitted and when it reaches the destination point. In order to protect sensitive medical data, the principles of "need to know" and relevance apply. Under this premise users should be allowed to access a patient's EHR in order to obtain the relevant information to carry out a task in concordance with the access and security policies of the organization in which the patient has been treated (Blobel, 2004; Garson & Adams, 2008). The principle of need-to-know is driven by the relevance that the accessed information has in the support of the patient care. However, relevancy is an ambiguous concept that depends on the context in which the information is generated and the purposes for which the data has been released. Consequently, the information accessed by a physician should be relevant but also sufficient to provide health care services (van der Linden, Kalra, Hasman, & Talmon, 2009).

Securing medical information is not only a social, ethical and technological matter, but is also about the establishment of well defined privacy policies and legislation. The legal duty of confidentiality is embedded in the professional relationship between physician and patient, and therefore, an essential aspect to be considered when exchanging medical records. From a perspective in which the mobility of patients as well as the exchange of information becomes more usual, the definition of means to protect the privacy and confidentiality of the patients in an efficient way becomes even more necessary. Both security services and mechanisms are essential for allowing access to authorized users as well as for protecting sensitive medical information during the exchange of data (Blobel, et al., 2006). Therefore, it is essential for health information systems to consider both the protection and privacy of patient's data but also the safe and authorized retrieval of information. At this point, it is important to consider that adding excessive security measures could lead to an inefficient, more time demanding and less user friendly access control methods. Defining the correct balance between security requirement and availability of information is a critical goal in a complex environment such as health care (Lopez & Blobel, 2009).

## Security and privacy in a shared care paradigm

In a shared care environment, different health care units (HCU) are involved in the care process as well as in maintaining accurate medical records. Indeed, in modern healthcare environments different care services are offered by different HCU within the organization or in a healthcare network that involves multiple organizations. This requires the communication and cooperation among all actors involved in the administration of patients' care (Choi, et al., 2006). Internet turns into a natural environment for such functionalities by allowing the exchange of EHRs and the interconnection of medical applications, thus facilitating better management of medical services as well as faster treatment of patients (Gritzalis & Lambrinoudakis, 2004).

As in paper-based health records, physicians have an ethical obligation of protecting patient information in order to prevent potential harm to an individual. Nevertheless, the nature of EHRs has transformed the duty of physician-patient confidentiality to a complex task. Despite the personal nature of health records, EHRs make patient's information potentially available to anyone with access to a health information system (Anderson, 2007). Therefore, the responsibility of protecting patient privacy has moved from an individual/local responsibility to a duty shared among the different entities that share the information. This tendency is altering the preexisting conception of the doctor–patient confidentiality and is threatening the quality of health care (Choi, et al., 2006). These apprehensions are also shared by the public whose primary concern is the security, privacy, confidentiality and protection of their personal health information (Goldschmidt, 2005; Rash, 2005).

In a shared care paradigm defining what is considered sensitive information as well as what access permissions are granted to users become uncertain. In fact, each participating institution of a health network would have different approaches for defining the level of sensitivity associated to the information, access rights and the level of security required to protect privacy of patients (Blobel, et al., 2006). Those approaches not only depend on legal restrictions but also are built based on the accumulated experience and the culture of organizations. Since the conception of security and protection of patient's privacy differ from one organization to another, methods for interconnecting health information systems should include comprehensive understanding of the complexity of requirements involving the secure exchange and release of medical data. In general, an electronic health record system able to secure and protect the confidentiality of patients should not only incorporate security requirements but also guarantee the flow and availability of the information.

Implementing a shared care environment has several implications not only in how the information is managed or which technology can be used but also in the way in which information is collected, stored and accessed. The exchange of information in a shared care environment exceeds the needs of a locally integrated health information system and requires the definition of a new set of requirements. Even more, it requires a different approach to overcoming the technical, legal and ethical issues that rise from exchanging highly sensitive information. In a shared care paradigm, the number of specialist that can have access to EHRs increases and the information contained by EHRs can be broken down among different health information systems within the organization or among different healthcare providers, increasing the possibility of a security breach. In general, the implementation of the share care paradigm not only requires the support of standardized information systems architectures, data exchange protocols and common vocabularies but also protecting the privacy of patients, guaranteeing the authorized access to stored data and protecting the integrity of the information (Blobel, et al., 2006).

## Securing the exchange of EHRs

Secure exchange and disclosure of electronic health records over insecure channels such as internet requires the implementation of comprehensive security policies and technologies that allows the exchange of data whilst the protection of patient's privacy is guaranteed (Choe & Yoo, 2007). These policies and technologies should provide mechanisms for access control and define access privileges for information management and protection of data privacy (Blobel, et al., 2006; Ohno-Machadoa, et al., 2004). During the electronic exchange of medical data, patient's sensitive information always has to be protected; especially the information considered sensitive due to the legal and ethical consequences that unauthorized releases could carry. The unauthorized access and release of sensitive information are considered a breach of confidentiality and could lead to issues of public concern such as discrimination, embarrassment or economic harm (Ohno-Machadoa, et al., 2004). At this point, several issues have to be considered: (1) the origin of the information, (2) the reason for its release, (3) secure transmission of data and (4) protection of patient's privacy.

The origin of the information refers to who and where the data has been collected. Health information can be collected by different organizations and can serve a variety of purposes, and its storage can be local or external. Information locally stored can be promptly available and can normally be accessed by user at any time and location within the organization. On the contrary, external health data is usually retrieved from information systems that do not provide direct access rights to users. In this case, access rights are provided based on common agreements between the organizations involved (Lopez & Blobel, 2009; van der Linden, et al., 2009).

The reason for the disclosure of information is an important element in defining an efficient security strategy. Detailed and grained information is normally required to offer primary services such as the treatment of a subject of care. On the contrary, information required for secondary uses should not be linkable to the patient (Agrawala & Johnson, 2007). The destination of the information also affects the definition of a security strategy. Local security needs substantially vary from the requirement of a shared care scenario (van der Linden, et al., 2009). Locally, standard security measures and standardized messages allow the secure access and disclosure of information. However, the secure exchange and release of information among different health providers not only depends on secure and standardized electronic mechanisms but also on standardized security and access policies (Lopez & Blobel, 2009).

# PROTECTING PATIENT'S PRIVACY AND CONFIDENTIALITY

## Social, ethical and legal perspective

The benefits of electronic health records and how the use of this technology could impact in society are still open for debate. Nonetheless, the general perception is that incorporating EHRs to medical practice provides support in the delivery of health care by facilitating access to historical medical data (Agrawala & Johnson, 2007; Anderson, 2007). EHRs provide an instrument to maintain non-fragmented and actualized health information.

The information collected in EHRs has a historical character and correspond to the lifelong medical records of an individual. A perfect EHR would be a complete health history of the patient's encounters with health system (Berner, 2008). However, having the complete medical history raises concerns over how the confidentiality of the information would be protected.

Traditionally, protecting the confidentiality of the information has been the responsibility of the physician and/or the institution that holds the patient's medical records. In a shared care setting, the provision of health care services becomes a multitask activity in which the interaction of multiple actors is required not only for providing health care but also in protecting the confidentiality of health records.

Under this complex scenario countries such as U.S., Canada, Japan and the member of the European Union have incorporated laws and regulations that aim to reduce fraud and abuse as well as protect patients' information (Anderson, 2007). International regulations such as that imposed by HIPAA (Health Insurance Portability and Accountability Act) and the European Data Protection Directive (Agrawala & Johnson, 2007; Lusignan, et al., 2007) demand the highest level of security and protection during the access, processing and exchange of information that involve sensitive data of individuals. Australia also possesses a set of privacy principles that regulates the collection, use and disclosure of personal information. Additionally, Australian legislation protects and provides a legal body for people that have suffered harm as a product of unauthorized disclosure or use of private information.

## Challenges of Securing Electronic Health Records

Securing electronic health records, in a scenario where information is potentially accessed by multiple actors, could become a complex and costly activity. To provide a framework for secure maintenance and release of health care information, the European Committee for Standardization has released a set of information security standards for health information systems (CEN-ENV, 2000a, 2000b, 2000c). CEN standards recognize four global security needs that any health information system should accomplish Availability, confidentiality, integrity and accountability (CEN-ENV, 2000a).

Availability of the information is a key factor for functional electronic health record systems; users with the right to access information should be allowed to do so in order to perform their duties. However, to protect the confidentiality of the information, access to patient's data should be carried out under the principles of relevance and need-to-know (Garson & Adams, 2008). The principle of relevance prevents the information overload and protects the patient's privacy by restricting the release of information to the relevant data required to support the health care process (Berner, 2008; van der Linden, et al., 2009). In the same way, the principle of "need-to-know" guarantees that only personnel who required the information and have the access privileges will be allowed to extract the data. Defining the correct balance between availability and security requirement of information is a critical goal in a complex environment such as health care.

A security breach poses a threat for protecting the integrity of electronic health records as well as for providing reliable information for accountability purposes. Integrity of the information is not only guaranteed by incorporating additional security mechanisms within the system or for securing a communication channel, when information is exchanged between systems, but also by ensuring that only authorized user can have access, add or alter stored data. In shared care environment controlling who is accessing the information turns into complex and time demanding task. Indeed, the solo fact that existing authentication methods, such as PIN or passwords, allows unauthorized delegation of access permissions threaten the integrity and validity of the information (Heckle & Lutters, 2007; Shin, et al., 2008). Accountability of information also becomes less accurate when non-authorized users are able to access and manipulate data regardless of the fact that they do not have the privileges to execute such activities.

## Analysis of traditional methods

In a shared care context the concepts of privacy, confidentiality, and security become essential for secure exchange of electronic health records. To provide a secure, safe and reliable environment for co-operation and communication, several security requirements need to be taken into consideration. Security may not only consider the services that will be implemented to avoid the unauthorized access to sensitive information but also mechanisms that prevent unauthorized release of patient's data.

Existing authentication and access control models require safekeeping PINs, passwords or smartcards in order to provide access to restricted facilities and information. However the nature of the activities executed by physicians and medical personnel requires mobility and multiple accesses to different terminal within the organization or even remotely in the case of web based health information systems or integrated multi-domain systems (Garson & Adams, 2008; Shin, et al., 2008). Considering that access to different systems may require multiple authentication methods, it is usual to find that PINs and passwords are maintained stored on the computer terminals used by physicians, stick papers on the office, laboratories, medical consult or at home, or become a simple combination of well known numbers or digits such as phone extension, date of birth or pseudonyms which are easy to remember but also relatively less efficient in avoiding security breaches (Garson & Adams, 2008; Shin, et al., 2008). The use of smartcards also may present certain disadvantages such as deterioration and accidental lost. Additionally, if physicians forget their PIN/passwords or misplace their smartcards a reissuance process must take place (Shin, et al., 2008). Consequently, existing models become inappropriate and less reliable for a medical environment.

Other issue associated to the use of traditional model is medical disputes generated by delegation of authentication codes (Chen, et al., 2008; Heckle & Lutters, 2007). Delegation of private authentication codes is generated when a member of a hospital's medical staff delegates his PIN/password or other authentication feature to other physician or nurse to access, modify or add information on behalf of the owner of the private authentication codes (Heckle & Lutters, 2007; Shin, et al., 2008). The delegation of access rights may grant access to sensitive information to non-authorized user by breaking established policies of information privacy and confidentiality (Heckle & Lutters, 2007; Shin, et al., 2008). This also may have legal repercussions when restricted information is leaked to third parties without the proper authorization of the patient or when the addition of erroneous information compromises the safety of patients.

## Traditional Access control models

In the following pages traditional access control models, such as DAC, MAC, RBAC, will be presented. In order to do so, a paradigm will be used (see Figure 1), where a doctor needs to acquire information regarding a patient's medical history from another institutions in order to handle the patient's case. Figure 2 presents a graphical representation of the relation and flow of information of the actors historically involved in the treatment of patient A described in Figure 1. The paradigm used presents difficulties that arise in providing health care in today's interconnected medical environments. These difficulties require efficient access control mechanisms in order to ensure security, for example, in the scenario discussed only doctor 'DC' who has the patient's consent accesses the patient's medical data. Traditional access control models try to cope with these kinds of difficulties giving access to a patient's EHR only to the rightful owner.

68 years old lady 'A' was admitted to the hospital 'HA' with abdominal pain and doctor 'DC' has been assigned to her case. The patient has indicated having a history of chronic diseases. 'A' has been previously hospitalized at hospital 'HB' for chest pain and followed up treatment with the cardiologist 'C' for Atrial Fibrillation, Hypertension and Recurrent Angina, also radiological information of the patient are maintain in the hospital records. Additionally, she has been diagnosed with diabetes for 20 years and has been visiting clinic 'CL' for her regular medical treatment. She has checked her blood according to the doctor's order at the local pathology 'P' regularly. 'A' has also been seen by the Dietitian 'D', Ophthalmologist 'O', podiatrist 'PO', Exercise Physician 'EX' for her diabetes and diabetes related complications. She visited gynecologist 'G' for postmenopausal symptoms 2 years back and had an episode of knee pain 3 weeks ago having taken an x'ray at the Radiology 'R'. She is on several medications for different conditions. As an elderly lady with multiple pathologies, the doctor 'DC' has decided to trace back her history from her healthcare providers. The patient has also given consent for the doctor to do that.

*Figure 1: Case Analysis*

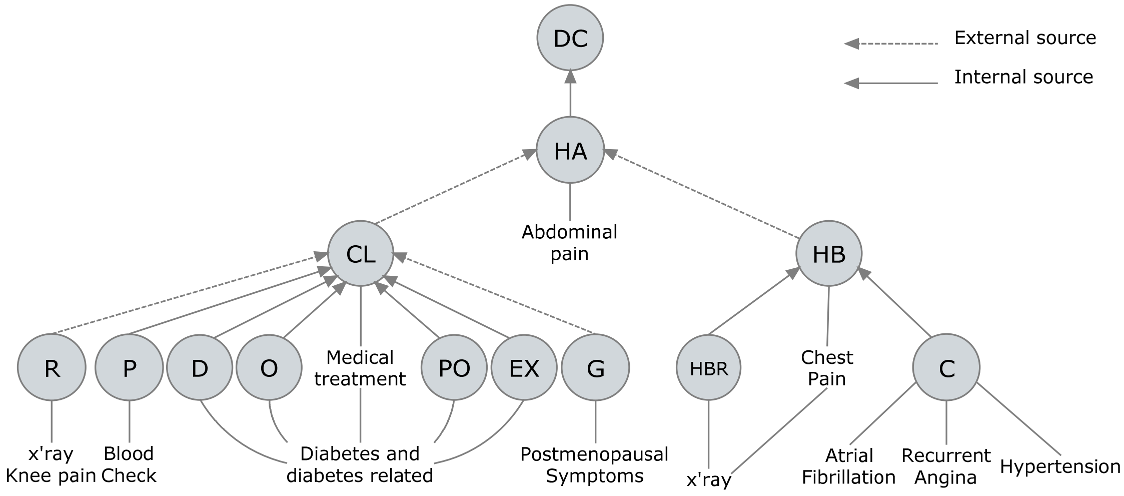

*Figure 2: Case analysis, interaction and expected flow of information*

**Mandatory Access control**

Mandatory access control polices (MAC) govern access based on classification of subjects and objects within a system. The access control decision is made by a centralized authority that determine, on one hand, the level of security required for each object and, on the other hand, the trustworthiness level of subjects for accessing the protected information (R. S. Sandhu & Samarati, 1994). Access control is based on comparing security levels, which indicate how sensitive data is and is performed by assessing security clearances, which indicate the entities that are allowed to access such data. To access the information a subject should have at least a level of security clearance equal to the security level of the object being accessed (Stallings & Brown, 2008). MAC policies established that users cannot delegate access rights in this way enforcing protection of the data “level”, this guarantees the confidentiality of the accessed data (Stallings & Brown, 2008). MAC policies also allow the establishment of fine-grained access rights over data and, at the same time, reinforce established access restrictions. However, MAC policies are rather rigid which make them unsuitable for a shared care environment, especially considering that in MAC more than one security level cannot be assigned to the same data object (Hafner et. all, 2008).

For example, in our previous mentioned paradigm, a situation where information of patient 'A' is maintained under MAC policies, doctor 'DC' will be required to provide the necessary clearances to retrieve the data from clinic 'CL' and hospital HB information systems. In this case, the data fields confining patient 'A' information would be maintained labelled with different levels of security accordant with the sensitivity of the information. Doctor 'DC' would be able to retrieve the data that reflect the access right provided by the clearances that he possesses. In fact, to maintain the principles of need-to-know and relevance 'DC' would only have access to the relevant information needed to perform the task. However, a physician with the same security clearances to 'DC' would also be allowed to access the retrieved data, which would not reflect the consent provided by patient 'A' to doctor 'DC'. MAC policies are centered on the level of sensitivity of the information rather that rights and permissions that users or user groups have to access the data, which does not allow discriminating among users with the same clearances.

Furthermore, in a shared care context where data can be exchanged between multiple organizations, delegated and accessed by multiple users in a need-to-know base, users can play different roles and have access to information under different contexts (Alhaqbani & Fidge, 2008). However, delegation of information and establishing hierarchies of access permissions are not allowed by MAC policies. In general, although MAC policies are less complex to define and allow the establishment of fine-grained access permissions based on the sensitivity of the information, they are extremely rigid for a health care environment, especially in managing users and user groups and delegation of access permissions (Hafner, Memon, & Alam, 2008)

### Discretionary access control

Discretionary access control (DAC) is based on the identity of the requestor (user or system process) and on access rules, which establishes what the requestor is allowed to do. Access will be granted to the user accordantly to the permissions that the user has over the object at the moment of accessing it. DAC policies allow users to provide access permissions to another entity (user or system process). However, they do not impose restriction on how information will be managed when it is received by a user. In fact, a user could pass the data to another user not authorized to access it.

A key element of DAC is the ownership of the information, especially because owners are allowed to grant access to the stored data. However, in health care ownership of the information is not always clear. In fact, EHRs belong to a patient but are created and modified by health care professionals and the information is not only shared but also could be maintained by different health organizations which could claim ownership of the data (Alhaqbani & Fidge, 2008; Hafner, et al., 2008). Considering the situation of patient 'A', the data retrieved by doctor 'DC' from clinic 'CL' and Hospitals 'HA' and 'HB' correspond to her personal health information; however ownership of the data is not clear. In the case of patient ‘A’, contents of her electronic health records have been created and accessed by physicians of the three organizations as well as information has been collected from other external sources (radiology results and postmenopausal symptoms in the case of clinic 'CL'). Additionally, patient 'A' electronic health records is distributed in the information systems of all three organizations that, in principle, would have different access principles and security policies. The example shows that information could be created by various collaborative partners that could not claim complete ownership of the data.

Although, access policies are flexible, the model lacks the ability of supporting dynamic change of access rights. Additionally, fined grained access privileges are difficult to be managed, especially when users are allowed to grant access right to other users. DAC is centered in users rather than user groups; however, if the model is extended by including categories or group definitions, group management is possible.

In general, DAC policies are less complex to implement if compared to RBAC, they are also flexible but still restricted for a shared care environment and increase the complexity of defining fine-grained access to stored data. Implementing DAC in shared care settings could result in additional security problems (R. S. Sandhu & Samarati, 1994; Stallings & Brown, 2008).

## Role-based access control and exchange of EHRs

Most of the existing researches consider role-based access control (RBAC) as a mechanism to guarantee authorized access to electronic health resources, especially during the exchange of EHRs. Role-based access control (RBAC) is used to protect information resources from unauthorized access based on the roles that user could have or perform within an organization. RBAC was first introduced by David Ferraiolo and Richard Kuhn in 1992 as a mean to provide manageable access privileges to identifiable groups of users (Ferraiolo & Kuhn, 1992). The Ferraiolo-Kuhn model was later integrated with the framework proposed by Sandhu et al.(R. S. Sandhu, Coynek, Feinsteink, & Youmank, 1996) and published as the NIST RBAC model in 2000 (R. Sandhu, Ferraiolot, & Kuhnt, 2000). The integrated framework proposed by Ferraiolo, Sandhu and Richard was adopted as ANSI/INCITS standard in 2004.

The central idea of the RBAC model is that users can perform multiple roles and roles can be associated to multiple access permissions. In RBAC permissions are represented by the relation existing between resources and operations over those resources (Lee, Kim, Kim, & Yeh, 2004). In practice, RBAC models are based on access policies defined in terms of permissions that are associated with roles assigned to users. Permissions will determinate the operations that a role is able to perform on information resources and, therefore, all users that have assigned that specific role (Kim, Ray, France, & Li, 2004).

Even though the RBAC model has been successfully implemented in several domains, in the healthcare it presents several issues that need to be considered. Some of these issues are described in the following situations which are described using the case presented in Figure 1.

### *Roles definitions*

Role can be defined based on the structure of the organization or functions that performs members within the organization. This could lead to an ambiguous definition of access permission that can generate security issues when information is exchanged among organizations. Since in RBAC models operations are generically assigned to roles, it is difficult to separate into individual access permissions. However, when the patient 'A' is admitted to 'HA', the assignation of the access permission is done based on the consent given by the patient and not by the access privileged that could be associated to roles. For example, the patient will be treated by Cardiologist 'CA-A' but not the Cardiologist 'CA-B'. Therefore, even though both Cardiologists could have the same role, only cardiologist attending A should be allowed to access the patient’s information. Furthermore, in a shared care environment the team of physicians taking care of patient A should be the only ones with access to his medical records. In this case roles are not sufficient to determine access privileges, but the function of the physician within the team or been part of the team. In reality access to the health information is given to the members of the 'team' treating the patient and not to all physicians with similar roles within the organization. Under these conditions, role-base access control will not provide a suitable solution to the problem of restricting access to those users that are not taking part of the patient treatment.

Since in role-based access control models access permissions are determined by the role assigned to a user, the control that the patient has over the access to specific and sensitive information will be intrinsically limited. In fact, in a conventional RBAC model patient A would not control whatsoever over permission assigned to his medical records.

### Combining and extending Access control models

Alhaqbani and Fidge proposed a security access control protocol based on a three level access security model (Alhaqbani & Fidge, 2008). The proposed protocol combines Discretionary Access Control (DAC), Mandatory Access Control (MAC) and Role-Based access control in hierarchically layered security mechanism, which determine access to data depending on a set of rules and policies evaluated at each level. According to the access hierarchy of the model, access to sensitive information will be determined by a Mandatory Access Control Policy, which provides a solution to the previously described scenario. However, implementation of this model in a shared care environment would be rather complex. The complexity of EHRs would limit the usability of DAC in a shared care setting since role definition can differ among health providers. Moreover, the complexity of all models could be reduced by reinforcing the policy that allows/restrict access to information stated as sensitive.

Motta and Furuie proposed a Contextual Role-Based Access Control (C-RBAC) model which extends the conventional RBAC definitions by including contextual information to determine access permissions to patients’ data (Motta & Furuie, 2003). In this case, the model allows the statement of pacific restriction by adding contextual data to restrict the access to the information. Context information such as physicians assessing of patient, location and time can be used to determine if a user can be granted with access to information. The model was developed to be flexible in granting fine-grained access privileges in large health care centers using RBAC. Nonetheless, its definition and structure limits the model to local environments, which made the model unsuitable for shared care environments with participation of multiple health care providers.

Peleg et. al proposed a solution based on contextual RBAC which considers definition of scenarios, which are called situations, in which user would be allowed to access EHRs. Situations are described and classified, and each classification would define a pattern that can be applied when a user is requesting access to information (Peleg, Beimel, Dori, & Denekamp, 2008). The Situation Role-Based Access Control (S-RBAC) model could also be used to manage access permissions over remote repositories by applying patterns that define situations in which inter-institutional exchange of information is allowed. However, the model was developed using a patient centric approach which did not directly consider requirements of all possible stakeholders. Additionally, since the model is based on RBAC, conflicting roles and access policies would be expected when data is exchanged among different health care providers, which will increase the complexity in defining situational patterns for data exchange and release. Also, if additional health providers and all possible stakeholders scenarios are described and included, the number of pattern would potentially increase as well as the complexity of managing access permissions.

*Table 1: Comparison of access control policies*

| | **MAC** | **DAC** | **RBAC** | **C-RBAC** | **S-RBAC** |
|---|---|---|---|---|---|
| Complexity | Low | Low | Medium | High | High |
| Multiple users | Restricted | Restricted | Possible | Possible | Possible |
| Policy management | Rigid/Restricted | Flexible/Restricted | Applicable | Applicable | Applicable |
| Fine-Grained access | Applicable | Restricted | Restricted | Applicable | Applicable |
| Pros | Guarantees protection over accessed data<br>Allow Fine-Grained access restrictions | Policies are Flexible | Allows management of access right at group level<br>Facilitate the management of access right in large organizations | Considers the contextual information to determine fine-grained access to medical records | Considers the contextual information to determine fine-grained access to medical records<br>Is designed for share care settings |
| Cons | Protection policies are centered on the information rather that user or user groups.<br>Difficult to implement in large organization with multiple user and groups accessing the data | Establishment of ownership over the data is rather difficult in shared care environments.<br>The model lack the ability to support dynamic change of access right<br>It is limited and difficult to manage in a shared care scenarios | Lacks the ability to specify fine-grained access right for users<br>Constraints are not flexible<br>Different role definitions could be present when information is exchange among health providers | Is not designed for share care settings | Model is patient is mainly patient centered, and does not consider all stakeholders<br>Level of complexity potentially increase with the inclusion of additional situations<br>Different role definitions could be present when information is exchange among health providers |

## Attribute-Based Encryption

Attribute-based encryption (ABE) has its origins in Identity-Based Encryption (IBE) schemes, firstly proposed in (Boneh & Franklin, 2001). The IBE scheme allows a sender to encrypt a message using an identity without incorporating a public key infrastructure (Sahai & Waters, 2005; Shamir, 1985). In this case, the identity is viewed as a string of characters (e.g. user's name, an email address, or telephone number) which serves as a user's public key (Liu, Guo, & Zhang, 2009). A private key, which is provided by a trusted private key generator (PKG), is used to decrypt the data. The private key is provided only if the user has been successfully identified by the PKG (Au, et al., 2008)

Sahai and Waters (Sahai & Waters, 2005, 2008) introduced the notion of attribute-based encryption (ABE) as a new mechanism for reinforcing access control. The attribute-based encryption approach allows a ciphertexts to be decrypted by more than one recipient, unlike the traditional public key cryptography methods (Bethencourt, Sahai, & Waters, 2007). In its place, both the users' private keys and ciphertexts are associated with a set of attributes or policies that are used to grant access to the encrypted data. Attributes are defined as set of strings, in this case represented by access policies, which are associated to an access structure applied to the encrypted data. A user would be able to decrypt an encrypted data only if he/she possesses a private key with attributes that overlap the attributes used in the ciphertext (Bethencourt, et al., 2007; Ibraimi, Tang, Hartel, & Jonker, 2009). In other words, to allow a user to decrypt a ciphertext, at least *k* attributes must overlap between the identity used to generate the ciphertext and his private keys. Note that not all but *k* attributes are sufficient to grant access to the encrypted data, which is represented as an error-tolerance in the model (Sahai & Waters, 2008). This error-tolerance allows the implementation of Fuzzy Identities or Attribute-Based Encryption schemes for biometric technology (Sahai & Waters, 2005).

In this section, we will present and describe an Attribute-Based Encryption scheme and how it can be applied to protect the information of parties during the exchange and release of EHRs.

## An approach for securing EHRs exchange and applications

Considering the case in Figure 1, Hospitals 'HA', 'HB' and Clinic 'CL' have previously agreed in a set of principles that allow them the exchange of information. Those principles have been set on contracts that permit the transference of any relevant data regarding health history which can be required during the treatment of a patient. All institutions have defined independent security approaches and mechanism for protecting the information that is managed on their system, HA and HB being public hospitals and according to the health policy guidelines for a public hospital, CL, being a General Practice, following the guideline for security from the General Practice Computing Group. Therefore, there could be differences in access control, security and information release polices. To avoid controversies policy reinforcing method is used during the exchange and release of information. The method proposed is reinforcing security policies by using attribute-based encryption scheme. In this case, the access policies are used to encrypt the information that has been exchanged, allowing only users with the correct access privileges to decrypt and access the information.

### Data Encryption

Considering the scenarios described previously, the exchanged information is maintained encrypted until an authorized user, with the sufficient *k* attributes, proceeds to decrypt the message completely or partially. In this case, a secret key, *SK*, is used to decrypt the ciphertext encrypted with the initial attribute set (access policies), *Ap*, if and only if the attributes that the user possesses are sufficient as measured by the “set overlap” distance metric for the security policies used to encrypt the data (Sahai & Waters, 2005). To decrypt the message, a private key is also needed. The scheme requires of a trusted authority, known as the Private Key Generator (*PKG*), with the task of generating the private key (*SK*). The *PKG* will provide such a private key only after the user has been successfully identified (Au, et al., 2008). The generated key can then be used to decrypt the ciphertext originally received from the sender (see Figure 3). In the following, *k* denotes the minimal number of attributes that the user must have in order to decrypt the message or part of it.

This approach guarantees that only users that have access privileges would be allowed to access the encrypted data. The access privileges are described by the security policies used to encrypt the data. A user that does not have the attributes required to decrypt the data will not be able to access the information. If the security policies attached are hierarchically associated to information, the access could be provided at different levels for different users. In this case, user will be able to access different level or contents within the encrypted data depending on the attributes associated to their access privileges.

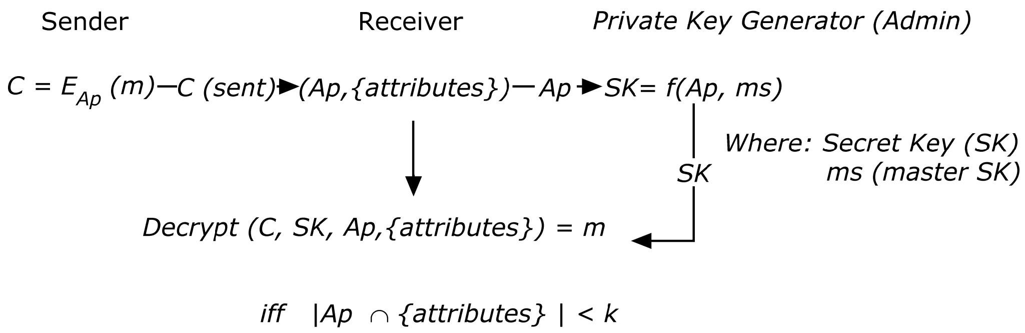

*Figure 3: Attribute-based encryption*

**Enforcing of access control policies and secure transference of data**

*Information exchange*

After patient A is admitted to hospital 'HA' and her first encounter with physician 'DC', doctor 'DC' starts recollecting patient 'A' historical medical data. The recollection starts with the remote request of data from clinic 'CL' and hospital 'HB' health information systems. To guarantee the confidentiality of the information, the data is encrypted using attributes associated to physician 'DC'. Since the transference of data is done by reinforcing access policies only doctor 'DC' will initially be authorized to decrypt the data provided by clinic 'CL' and hospital 'HB'. Considering that patient 'A' will not only be treated by physician 'DC' but also by a team of physicians and medical staff, the access permissions will eventually be modified in order to provide access to all personnel involved in with patient’s 'A' care. This can be done by providing a private Key to each member of the staff assuming responsibility with patient’s 'A' care; each member will be allowed to retrieve the information depending on the described access policies described by the attributes associated to their private keys. For example, physician treating patient 'A' will have access to all relevant medical history of the patient, on the contrary nurses and administrative staff would be provided with restricted access to the data.

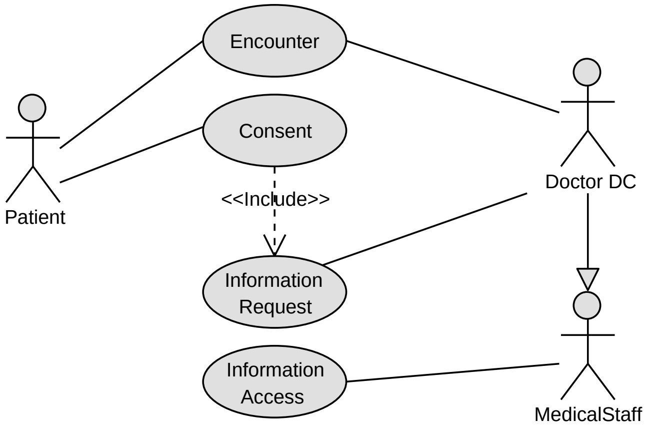

*Figure 4: Case use Scenario 1*

*Analysis*

This case presents a normal patient-physician encounter in which the historical information of patient A can only be accessed by the primary physician at hospital 'HA' by Doctor 'DC'. To simplify the analysis let us assume that the consent policy has been created during the first encounter (steps 1 and 2 in Figure 6). As it has been described previously, the policy defines a set of attributes that establishes who would be able to access the medical information of patient A. In this case a set of attributes *({Pat.A},{Doc.GP, Clinic.CL})* is used to describe the access permission to patient A's information.

Even when the patient has progressed through the health system, the information gathered from the counter, encounters and reports can be shared using electronic communication. An information request made by doctor DC would start the process as shown in steps 3 and 4 of Figure 6. The information in the EHRs of hospital 'HB' and clinic 'CL' can be encrypted using the attributes (*{Pat.A},{ Doc.DC, Depto.ME, Hosp.HA })* and send directly to the electronic health record system in hospital HA, which is shown in steps 5 and 6 of Figure 6. In this case the access policy for the data is described as $M_{(data)} = (Pat.A) \vee (Doc.DC \wedge Depto.ME \wedge Hosp.HA)$. Since patient cannot possess a private key that includes the attributes *{Doc.DC, Depto.ME, Hosp.HA }* the access tree has only two possible outcomes.

$$P_{(Mrpitt)} = (Pat.A) \vee (Doc.DC \wedge Depto.ME \wedge Hosp.HA)$$

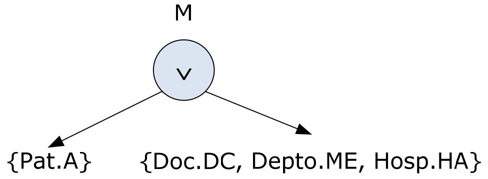

*Figure 5: Access tree Patient's Data*

In this scenario, the transfer of information is directly managed between sender ('HB' and 'CL' information systems) and receiver (Doctor 'DC'). Since the information is shared between organizations the attribute { *Doc.DC, Depto.ME, Hosp.HA* } is applied to encrypt the relevant medical information associated to patient A, and then sent to the HA's information system.

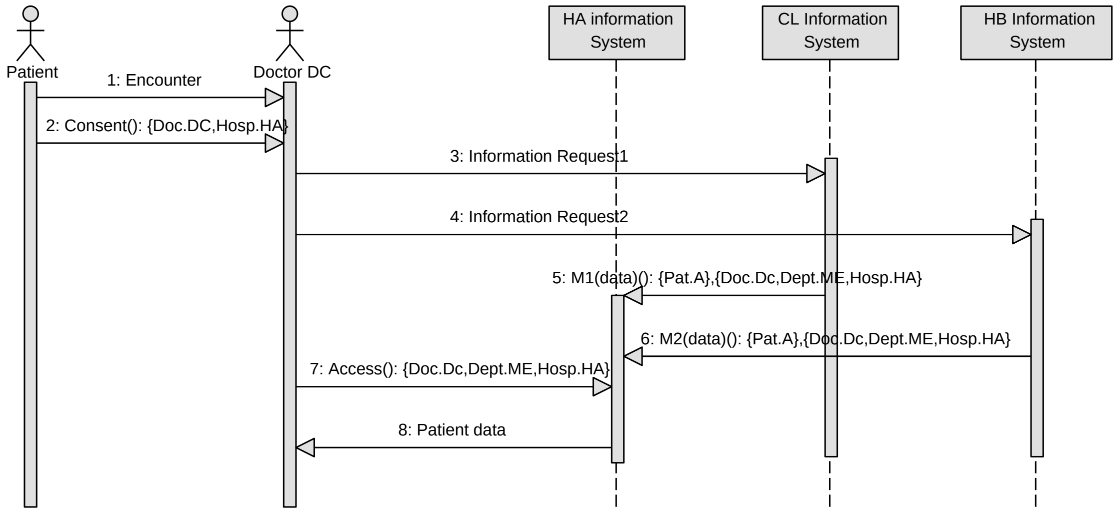
Patient
Doctor DC
HA information System
CL Information System
HB Information System
1: Encounter
2: Consent(): {Doc.DC,Hosp.HA}
3: Information Request1
4: Information Request2
5: M1(data)(): {Pat.A},{Doc.Dc,Dept.ME,Hosp.HA}
6: M2(data)(): {Pat.A},{Doc.Dc,Dept.ME,Hosp.HA}
7: Access(): {Doc.Dc,Dept.ME,Hosp.HA}
8: Patient data

*Figure 6: Sequence Diagram Scenario 1*

The information collected and sent directly to the 'HA' systems, can be accessed by 'DC', as it is illustrated in steps 7 and 8 of Figure 6. At this point, the transferred data has been protected using an enforced access policy approach; therefore the information can only be accessed by Doctor 'DC'. To provide access to other members of the staff access permissions can be modified by associating new access key to the encrypted data. For example, by allowing Cardiology 'CA-A' to have access the patient medical history. This delegation of access to specific users is possible because attribute-based encryption supports partial delegation of access permissions. To enforce that only 'CA-A' is able to access the data the information the following attributes will be incorporated to the access permissions ({ *Doctor.DC, Depto.ME*}).

*Access delegation and patient control over data access*

Now consider the situation presented in role definition. According to the access and security policies of hospital 'HA' only member of the team attending the patient can have access to his EHRs. Since originally the information was requested and collected by doctor 'DC' of Medicine department the data could be encrypted using the flowing attribute set $M_{(data)}= (Pat.A) \vee (Doctor.DC \wedge Depto.ME)$. However, to allow other physicians access to patients 'A' data, a new set of attributes need to be incorporated. In this case, physicians could be provided with private key and assume specific responsibilities, which are described by a specific set of attributes (policies). Additionally, information could restrict in some specific cases, which can be described by a specific set of attributes (policies). Each specialist will be able to decrypt the data, which is under his responsibility, but will not be able to decrypt the data that has been restricted. This provides a solution for restricting access only to members of the team treating the patient and to patient's control over access permissions.

*Analysis*

Initially only doctor 'DC' has access to the patient information. To allow access to cardiology 'CA-A' a new set attribute can be added to the access policy of patient 'A', the new set will incorporate attributes set associated to 'CA-A'. Since cardiology 'CA-A' works the Cardiology department of hospital 'HA', the new set of attributes would be $M_{(data)}= (Pat.A) \vee (Doctor.DC \wedge Depto.ME) \vee (Doctor.CA\text{-}A \wedge Depto.CAR)$. No other cardiologist will have the attributes {*Doctor.CA-A,Depto.CAR*} associated to their access privileges, therefore no one else but CA-A will be allowed to access and manipulate patients 'A' data. The new access tree has only three possible outcomes:

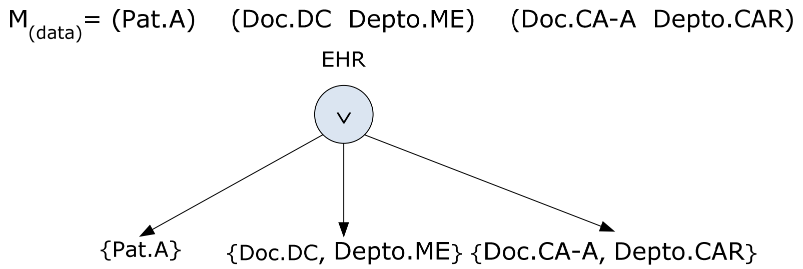
M(data)= (Pat.A)    (Doc.DC  Depto.ME)    (Doc.CA-A  Depto.CAR)
EHR
∨
{Pat.A}
{Doc.DC, Depto.ME}
{Doc.CA-A, Depto.CAR}

*Figure 7: Access tree considering access to cardiologist CA-A*

When patient A provides consent to Doctor 'DC' to collect his historical medical information, he could state that only physician involved in his case would have access to his psychiatric history, denying access to other physicians and personnel of hospital 'HA'. In this case the access Key of other physicians and personal will not allow them to access to the psychiatric history of patient 'A'. the access to the information is stated according to the consent of the patient and the access policies. The access then will incorporate the restrictions over information access, making some of the information unable to access for other physicians even when they could have access to the patient's EHR.

## CONCLUSIONS

Health information systems, in special Electronic Health Record (EHR), are considered crucial sources of information for healthcare professionals and an essential instrument for delivery of health care services. Nevertheless, the level of accessibility provided by health information systems raises concern over the secure access and release of information, especially in share care environments. In shared care context protecting the confidentiality of patients become the focus of attention and a key element to be considered in the implementation of information interfaces for data exchange among health care providers. Functional and reliable inter-domain EHRs require the consideration shared concepts as well as standardized terminology and standardized information architectures.

At the application level, the main security issue presented in approaches based on MAC and DAC approaches are inflexibility of the policies, complexity in determining ownership of the information, difficulty in implementing on large shared care environments and restriction considering delegation and hierarchical access permissions to the data. Implementation based on RBAC models present security issues associated to the ambiguities that exist in the definition of roles and access privileges among organizations, the non-existence of a common and/or standardized framework for defining roles and access privileges, lacking the ability of fine-grained access to information. Extensions to RBAC have allowed the fine-grained definition of access rights to data but at the same time increased the complexity of the models. The proposed approaches have failed to provide suitable solutions for exchange of date in scenarios that involve more than one health care provider.

In this chapter, we presented a security approach which reinforces access policies using attribute-based encryption schemes. Attribute-based encryption allows the encryption decryption of data based on polices, which are represented as attributes associated to the information. The approach allows an independent but secure method to protect the privacy and confidentiality of a patient information transmitted over insecure channels. The model is flexible in providing access to multiple users based on security policies, which describe the access permissions over encrypted data. The use of attribute-based encryption allows:

1. Control over access permissions of transmitted data: only user with the private access key that satisfy the encryption protocol will be able to decrypt the exchange information.

2. Delegation of access permission: Access to information can be delegated/granted to other users by providing an access key which satisfies the encryption protocols.

3. Protection of the patient's data: the transmitted information is encrypted in a fashion in which only users with the appropriate key will be able to decrypt the information. In addition, data can only be accessed when a user possesses the appropriate access permissions, and information is provided considering the principles of need-to-know and relevance.

4. Hierarchical access to rumpled data: User can access the complete information or part of it, depending of the attribute set associated to the private key.

In conclusion, attribute-based encryption offers several security advantages over traditional methods and also can be used for different purposes. In fact, it provides a flexible access control mechanism that can be implemented under different circumstances. Future work in this area is to explore and provide a suitable and scalable solution for complex health care environment. The complexity of modern EHR systems require flexible solutions that can be adapted in a variety of settings. In addition, the growing quantity and variety of the information collected by EHR systems along its potential uses demand scalable solutions. Moreover, in a shared care environment the number of interconnected systems and the potential numbers of users increase the demand for secure mechanisms that can cope with an increasing need for highly sensitive information.

## REFERENCES

Agrawala, R., & Johnson, C. (2007). Securing electronic health records without impeding the flow of information. International Journal of Medical Informatics, 76 471-479.

Alhaqbani, B., & Fidge, C. (2008). Access Control Requirements for Processing Electronic Health Records Business Process Management Workshops (pp. 371-382).

Anderson, J. G. (2007). Social, Ethical and Legal Barriers to E-health. International Journal of Medical Informatics, 76, 480-483.

Au, M., Huang, Q., Liu, J., Susilo, W., Wong, D., & Yang, G. (2008). Traceable and Retrievable Identity-Based Encryption Applied Cryptography and Network Security (pp. 94-110).

Berner, E. (2008). Ethical and Legal Issues in the Use of Health Information Technology to Improve Patient Safety. HEC Forum, 20(3), 243-258.

Bethencourt, J., Sahai, A., & Waters, B. (2007). Ciphertext-Policy Attribute-Based Encryption. Paper presented at the Proceedings of the 2007 IEEE Symposium on Security and Privacy.

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

Blobel, B., Nordberg, R., Davis, J. M., & Pharow, P. (2006). Modelling privilege management and access control. International Journal of Medical Informatics, 75(8), 597-623.

Boneh, D., & Franklin, M. (2001). Identity-Based Encryption from the Weil Pairing Advances in Cryptology — CRYPTO 2001 (pp. 213-229).

CEN-ENV (2000a). Health informatics - Security for healthcare communication - Part 1: Concepts and terminology. Published Standard CEN ENV 13608-1:2000: European Committee for Standardization.

CEN-ENV (2000b). Health informatics - Security for healthcare communication - Part 2: Secure data objects. Published Standard CEN ENV 13608-2:2000: European Committee for Standardization.

CEN-ENV (2000c). Health informatics - Security for healthcare communication - Part 3: Secure data channels. Published Standard CEN ENV 13608-3:2000: European Committee for Standardization.

Chen, Y.-C., Chen, L.-K., Tsai, M.-D., Chiu, H.-C., Chiu, J.-S., & Chong, C.-F. (2008). Fingerprint verification on medical image reporting system. Computer Methods and Programs in Biomedicine, 89(3), 282-288.

Choe, J., & Yoo, S. K. (2007). Web-based secure access from multiple patient repositories. International Journal of Medical Informatics, 1-7.

Choi, Y. B., Capitan, K. E., Krause, J. S., & Streeper, M. M. (2006). Challenges Associated with Privacy in Health Care Industry: Implementation of HIPAA and the Security Rules. Journal of Medical Systems, 30(1), 57-64.

Conrick, M., & Newell, C. (2006). Issues of Ethics and Law. In M. Conrick (Ed.), Health Informatics: Transforming Healthcare with Technology. Melbourne: Thomson Social Science Press.

Eddy, A. (2000). Critical Analysis of Health and Human Services' Proposed Health Privacy Regulations in Light of the Health Insurance Privacy and Accountability Act of 1996. Annals of health law, 9, 1-72.

Ferraiolo, D., & Kuhn, R. (1992). Role-Based Access Control. Paper presented at the 15th National Computer Security Conference, Balmy, Baltimore, USA.

Garson, K., & Adams, C. (2008). Security and privacy system architecture for an e-hospital environment. Paper presented at the Proceedings of the 7th symposium on Identity and trust on the Internet.

Goldschmidt, P. G. (2005, October). HIT and MIS: implications of health information technology and medical information systems. Communications of the ACM, 48, 68 - 74.

Grain, H. (2006). Consumer issues in Informatics. In M. Conrick (Ed.), Health Informatics: Transforming Healthcare with Technology. Melbourne: Thomson Social Science Press.

Gritzalis, D., & Lambrinoudakis, C. (2004). A security architecture for interconnecting health information systems. International Journal of Medical Informatics, 73(3), 305-309.

Hafner, M., Memon, M., & Alam, M. (2008). Modeling and Enforcing Advanced Access Control Policies in Healthcare Systems with Sectet Models in Software Engineering (pp. 132-144).

Heckle, R. R., & Lutters, W. G. (2007). Privacy implications for single sign-on authentication in a hospital environment. Paper presented at the Proceedings of the 3rd symposium on Usable privacy and security.

Ibraimi, L., Tang, Q., Hartel, P., & Jonker, W. (2009). Efficient and Provable Secure Ciphertext-Policy Attribute-Based Encryption Schemes Information Security Practice and Experience (pp. 1-12).

Kim, D.-K., Ray, I., France, R., & Li, N. (2004, March 29 - April 2). Modeling Role-Based Access Control Using Parameterized UML Models. Paper presented at the 7th International Conference Fundamental Approaches to Software Engineering, FASE 2004, Barcelona, Spain.

Lee, G., Kim, W., Kim, D.-k., & Yeh, H. (2004, July 15-17). Effective Web-Related Resource Security Using Distributed Role Hierarchy Paper presented at the Advances inWeb-Age Information Management 5th International Conference,WAIM 2004 Dalian, China.

Liu, S.-l., Guo, B.-a., & Zhang, Q.-s. (2009). An identity-based encryption scheme with compact ciphertexts. Journal of Shanghai Jiaotong University (Science), 14(1), 86-89.

Lopez, D. M., & Blobel, B. G. M. E. (2009). A development framework for semantically interoperable health information systems. International Journal of Medical Informatics, 78(2), 83-103.

Lusignan, S. d., Chan, T., Theadom, A., & Dhoul, N. (2007). The roles of policy and professionalism in the protection of processed clinical data: A literature review. International Journal of Medical Informatics, 76, 261-268.

Motta, G. H. M. B., & Furuie, S. S. (2003). A contextual role-based access control authorization model for electronic patient record. Information Technology in Biomedicine, IEEE Transactions on, 7(3), 202-207.

Ohno-Machadoa, L., Silveira, P. S. P., & Vinterbo, S. (2004). Protecting patient privacy by quantifiable control of disclosures in disseminated databases. International Journal of Medical Informatics, 73(7-8), 599-606.

Peleg, M., Beimel, D., Dori, D., & Denekamp, Y. (2008). Situation-Based Access Control: Privacy management via modeling of patient data access scenarios. Journal of Biomedical Informatics, In Press, Corrected Proof.

Rash, M. C. (2005, April 4). Privacy concerns hinder electronic medical records. The Business Journal of the Greater Triad Area.

Safran, C., Bloomrosen, M., Hammond, W. E., Labkoff, S., Markel-Fox, S., Tang, P. C., et al. (2007). Toward a National Framework for the Secondary Use of Health Data: An American Medical Informatics Association White Paper. Journal of the American Medical Informatics Association, 14(1), 1-9.

Sahai, A., & Waters, B. (2005). Fuzzy Identity-Based Encryption Advances in Cryptology – EUROCRYPT 2005 (pp. 457-473).

Sahai, A., & Waters, B. (2008). Fuzzy Identities and Attribute-Based Encryption Security with Noisy Data (pp. 113-125).

Sandhu, R., Ferraiolot, D., & Kuhnt, R. (2000, July 26-27). The NIST Model for Role-Based Access Control: Towards A Unified Standard. Paper presented at the 5th ACM Workshop on Role Based Access Control, Berlin, Germany.

Sandhu, R. S., Coynek, E. J., Feinsteink, H. L., & Youmank, C. E. (1996). Role-Based Access Control Models. IEEE Computer, 29(2), 38-47.

Sandhu, R. S., & Samarati, P. (1994). Access control: principles and practice. IEEE Communications Magazine, v32(n9), p40(49).

Shamir, A. (1985). Identity-Based Cryptosystems and Signature Schemes Advances in Cryptology (pp. 47-53).

Shin, Y. N., Lee, Y. J., Shin, W., Choi, J., 110, P. s.-., & 10.1109/WAINA.2008.289, D. O. I. (2008, 25-28 March). Designing Fingerprint-Recognition-Based Access Control for Electronic Medical Records Systems. Paper presented at the INAW 2008 - 2nd International Conference on Advanced Information Networking and Applications - Workshops, Okinawa, Japan.

Stallings, W., & Brown, L. (2008). Computer security : principles and practice. Upper Saddle River, NJ: Pearson international ed

van der Linden, H., Kalra, D., Hasman, A., & Talmon, J. (2009). Inter-organizational future proof EHR systems: A review of the security and privacy related issues. International Journal of Medical Informatics, 78(3), 141-160.