Kent Academic Repository

Full text document (pdf)

Citation for published version

Ferreira, Ana and Cruz-Correia, Ricardo and Antunes, Luis and Chadwick, David W. (2007) Access Control: how can it improve patients' healthcare? In: Bos, Lodewijk and Blobel, Bernd, eds. Medical and Care Compunetics 4. Studies in Health Technology and Informatics (Volume). IOS Press, Netherlands, pp. 65-76. ISBN 978-1-58603-751-2.

DOI

Link to record in KAR

https://kar.kent.ac.uk/14578/

Document Version

UNSPECIFIED

Copyright & reuse
Content in the Kent Academic Repository is made available for research purposes. Unless otherwise stated all content is protected by copyright and in the absence of an open licence (eg Creative Commons), permissions for further reuse of content should be sought from the publisher, author or other copyright holder.

Versions of research
The version in the Kent Academic Repository may differ from the final published version.
Users are advised to check **http://kar.kent.ac.uk** for the status of the paper. **Users should always cite the published version of record.**

Enquiries
For any further enquiries regarding the licence status of this document, please contact:
researchsupport@kent.ac.uk

If you believe this document infringes copyright then please contact the KAR admin team with the take-down information provided at **http://kar.kent.ac.uk/contact.html**

KAR Kent Academic Repository

University of Kent

Access Control: how can it improve patients' healthcare?

Ana FERREIRA[abd], Ricardo CRUZ-CORREIA[cd], Luís ANTUNES[b], David CHADWICK[a]
[a]*Computer Laboratory, University of Kent*
[b]*LIACC- Faculty of Science of Porto*
[c]*Biostatistics and Medical Informatics Dept. of Porto Faculty of Medicine*
[d]*CINTESIS – Center for research in health information Systems and technologies*

Abstract. The Electronic Medical Record (EMR) is a very important support tool for patients and healthcare professionals but it has some barriers that prevent its successful integration within the healthcare practice. These barriers comprise not only security concerns but also costs, in terms of time and effort, as well as relational and educational issues that can hinder its proper use. Access control is an essential part of the EMR and provides for its confidentiality by checking if a user has the necessary rights to access the resources he/she requested. This paper comprehensively reviews the published material about access control in healthcare. The review reveals that most of the access control systems that are published in the literature are just studies or prototypes in which healthcare professionals and patients did not participate in the definition of the access control policies, models or mechanisms. Healthcare professionals usually needed to change their workflow patterns and adapt their tasks and processes in order to use the systems. If access control could be improved according to the users' needs and be properly adapted to their workflow patterns we hypothesise that some of the barriers to the effective use of EMR could be reduced. Then EMR could be more successfully integrated into the healthcare practice and provide for better patient treatment.

Keywords. Computer Security, access control, computerized patient record

Introduction

The widening use of healthcare information systems such as the Electronic Medical Record (EMR), which allows for the collection, extraction, management, sharing and searching of information, is increasing the need for information security (e.g. confidentiality, integrity and availability) [1], [2].

Although the EMR is a significant support tool for patients and healthcare professionals there are still some barriers that prevent its successful integration within the healthcare practice. These barriers comprise not only security concerns [3] but also costs, in terms of time and effort, as well as relational and educational issues that can hinder the proper use of the system [4], [5]. Relational issues may exist when, for example, the relationship between patient and physician is affected. Educational issues relate to the fact that healthcare professionals need to learn how to use and adapt the system to their own needs [6]. They are usually not consulted when the system is designed and implemented and therefore are most of the time forced to use the system and need to redesign their workflow patterns around it [5].

Access control is essential to provide for the confidentiality of the EMR because it is part of the authorisation process where the system checks if the user can access the resources he requested. The study of access control policies, models and mechanisms that are commonly used in healthcare and within the EMR can help us understand how access control can affect the success of EMR integration and how this can be used to minimize the barriers that are usually present.

The main objective of this paper is to review how access control has been studied, designed and implemented in general and compare this to similar research in the healthcare domain, more specifically within EMR systems. This review will help identify what are the main issues regarding healthcare professionals' needs in terms of access control, and identify the barriers that usually prevent the successful integration of access control systems into EMR. If the improvement of access control development and usage can reduce some of the EMR integration barriers then we hypothesize that patient treatment and support can be improved.

This paper is structured as follows. Section 1 briefly introduces the concept of access control and some of the complexities involved in its design and implementation. Section 2 presents some of the problems with EMR and how access control relates to them. Section 3 describes the methodology used for the review and section 4 presents the results obtained from the review. Section 5 analyses and discusses the results and suggests some ways to improve the design and use of access control and its integration with EMR in healthcare practices. Section 6 concludes the paper.

1. Access Control

Information security is usually defined by three main characteristics [2], [7]:

- confidentiality - the prevention of unauthorized disclosure of the information
- integrity - the prevention of unauthorized modification of the information
- availability - the prevention of unauthorized withholding of the information.

Confidentiality is often used interchangeably with privacy but they are not exactly the same. Privacy is the right of an individual to not have their private information exposed (and this is usually enforceable by law), whilst confidentiality is limiting access to information to authorised individuals only.

The complexity of building secure information systems relates mainly to three fundamental and competing factors: i) the complexity of the security technology itself, ii) the difficulty of classifying the information that is to be protected and iii) the use of the technology by humans. This last factor is normally the most problematic [8] because it deals with the interactions between humans and systems. Other important but secondary competing factors are: protecting information from unauthorised access whilst needing to be able to access it for audit or law enforcement purposes; and making it easy for an authorised user to gain access to the information but complex for an unauthorised user to do the same.

In order to securely access information within a system three steps are usually required: identification (where a user says who he is, e.g. with a login username); authentication (where a user proves his identification given in the first step, e.g. with a password or a PIN number); and authorisation (where access rights are given to the user). Whilst access control is conceptually part of the authorisation process that checks

if a user can access the resources he requested, we are including all three steps within the scope of our review since the first two steps are necessary precursors to the third. Furthermore many implementations combine the three steps together into one access control decision, by having the implicit access control policy that everyone who is successfully authenticated can have access to the resource. This is the coarsest granularity of access control policy, in which everyone has the same access rights. Thus the authentication mechanism becomes a combined authentication and authorisation mechanism.

The design of access control systems is very complex and should start with the definition of structured and formal access control policies as well as access control models [9]. An access control policy must describe the rules that need to be enforced in order to provide the information security requirements of the organization. Afterwards, an appropriate access control model must be chosen in order to model the rules defined within the policy. Examples of common access control models are: Role-Based Access Control (RBAC) that associates rights to groups of users according to their roles within the organization; Identity Based Access Control (IBAC) that associates rights to specific users depending on their needs; and Mandatory Access Control (MAC) that defines mandatory rules for all the users of the system. A model can also be hybrid and include more than one model in order to tackle the more heterogeneous needs of an organization. Only after the access control model is chosen can the right technology and both authentication and access control mechanisms be selected and implemented. Authentication mechanisms provide for the identification and authentication of a user to the system - the first 2 steps above - (e.g. login/password; fingerprint) while access control mechanisms protect against unauthorized use of the requested resources (e.g. access control lists, security labels) [10]. Both mechanisms should perform in a correct and consistent way according to the access control policy and model defined.

The means of providing access control has become more challenging as policies become more complex. These need to be studied carefully within the healthcare environment so that access control can be correctly developed and applied without hindering the system's use.

2. The Electronic Medical Record

Access control is of vital importance in healthcare. Confidentiality is a main concern when it is related to patient clinical information that needs to be private. It is essential to protect this information from unauthorized access and, therefore, misuse or legal liability.

The introduction of the EMR within healthcare organizations has the main goal of integrating heterogeneous patient information that is usually scattered throughout different locations [11], [12]. This is why the EMR is becoming an essential source of information and an important support tool for the healthcare professional. There is also an increasing need to access healthcare information at remote locations [13]. This and the distributed nature of the information stress the need for access control requirements to be taken seriously [14].

Although the EMR is an essential tool for the healthcare professional, the reality is that it still does not integrate easily and effectively with healthcare professionals' daily workflow and processes [15]. Several obstacles are mentioned by healthcare professionals concerning the use of EMR. The obstacles are associated with a concern

for patient privacy and other security vulnerabilities related to the easy distribution, sharing and wider online access of the information [16], [17].

Other barriers that prevent the successful integration and use of EMR are mostly related to human interactions with the system. These include the time taken by healthcare professionals to learn and to use the system, and the consequent extra time and costs the patients may incur if they have to wait longer to be seen and treated. In addition, relational and educational barriers also hinder the right use of the EMR. Relational barriers include the perceptions that the physician and the patient have about the use of the EMR and how their relationship can be affected by it. Educational barriers comprise the lack of proficiency and difficulties that healthcare professionals have whilst interacting with the EMR to perform their daily tasks [6].

Taking into account the problems mentioned above and considering that the main factor that is driving the integration of EMR systems is the need to improve clinical processes and workflow efficiency [13], a deeper understanding of how access control systems can affect this integration and how they are being developed within the EMR is required. This analysis is done in the following sections.

3. Methodology

In order to deepen the understanding of the design and implementation of access control systems, two reviews were performed. The first review comprised an analysis of the design and implementation of generic access control policies, models and authentication mechanisms, where the latter incorporated an implicit access control function, whilst the second review was similar but applied specifically to the healthcare environment.

3.1. Review for Generic Access Control

This review comprised full articles from the last 10 years (1996 until mid 2006) whose content covered generic access control policies, models and authentication mechanisms that incorporated an implicit access control function.

Searches were made in IEEE Xplore and ACM (Association for Computing Machinery) conference databases as well as SACMAT (Symposium on Access Control Models and Technologies) and ESORICS (European Symposium on Research in Computer Security). Specific queries were made in IEEE Xplore (access control<in>metadata) and ACM with “access control”.

The review method was done in several stages. We started by reading the titles and the abstracts from the list of articles retrieved by the queries. We tried to summarise in a table the most important topics about access control that we wanted to study. We included articles that described at least one of the following topics:

- **Type of access control policy**: Institutional, Legislation, End-user, override and other.
- **Type of access control model**: RBAC, IBAC and DAC, MAC, Hybrid and other.
- **Study and/or implementation**: Access control policy, access control model and Authentication Mechanisms with an implicit access control function.

- **Authentication mechanisms**: Login/password, Single Sign on, smartcard, fingerprint, digital signature, certificates and other.
- **Results**: Just build the model; prototype or real set implementation.
- **Problems**: The limitations.
- **Successes**: The advantages and benefits.

Articles that applied specifically to the healthcare domain were excluded from this review but included in the next one.

From the articles selected we tried to search the full articles and read them. The table was filled with the necessary information whilst the full articles were being read.

3.2. Review for Access Control in Healthcare

This review comprised full articles from the last 10 years (1996 until mid 2006) whose content covered access control policies, models and authentication mechanisms (that incorporated an implicit access control function) when applied in the healthcare environment.

Searches were made in medical databases such as Medline (that included the BMJ-British Medical Journal) as well as IEEE Xplore and ACM.

As one query was not sensitive enough several queries were made in Medline - “computer security access”, “access to information” and “security”, “access to information” and “confidentiality”; IEEE Xplore - (access control and health<in>metadata), (“access control' and health”<in>metadata), (access control and health<in>metadata), (pki<in>metadata) and patient; and ACM - "access control" and "electronic patient record" and "security" and confidentiality”.

The review method used was similar to the one presented in the previous section. We started by reading the titles and the abstracts from the list of articles retrieved by the queries. We tried to summarise in a table the most important topics about access control that we wanted to study. We included articles that described at least one of the following topics:

- **Type of access control policy**: Institutional, Legislation, End-user, override and other.
- **Type of access control model**: RBAC, IBAC and DAC, MAC, Hybrid and other.
- **Study and/or implementation**: Access control policy, access control model and Authentication Mechanisms with an implicit access control function.
- **Authentication mechanisms**: Login/password, single sign on, smartcard, fingerprint, digital signature, certificates and other.
- **Healthcare Institution**: Hospital, hospital department, primary care, private care and other.
- **Healthcare Information System**: EMR/EPR/CPR, prescription and consultation.
- **User Groups**: Medical doctors, nurses, patients and other healthcare professionals.
- **Portal/Internet access**: Healthcare professionals, patients and other.
- **Results**: Just build the model; prototype or real set implementation.
- **Problems**: The limitations.

- **Successes**: The advantages and benefits.

Next we tried to find the full version of the articles selected according to their titles and abstracts. The summary table was filled whilst the full articles were being read.

4. Results

The review results are presented below and analysed in section 5.

4.1. Review for Generic Access Control

351 articles were obtained within the search queries. After reading titles and abstracts 80 full articles were selected and read. Of these, 59 articles were deemed to be in scope and were included in the review.

As can be seen in Table 1, from the 17 articles that mentioned the definition and use of an access control policy only in 1 case was it implemented, and this was a prototype system. From the 59 articles that mentioned access control models, 52 concentrated on the study of an access control model and in only 8 cases were these studies implemented, mostly as prototypes with only 1 of these being implemented in a real scenario.

Table 1. No of papers reviewed covering access control policies, models and mechanisms between 1996 and 2006.

	1996-99	2000-03	2004-06	Total
Access Control Policy				
Study/Analysis		4	12	**16**
Implementation			1	**1**
Access Control Model				
Study/Analysis	4	11	37	**52**
Implementation		2	6	**8**
Authentication Mechanisms with an implicit access control function				
Study/Analysis		5	10	**15**
Implementation		1	2	**3**

The most commonly used access control model was RBAC, being covered in 38 articles out of 52. The most commonly studied and prototyped authentication mechanism was digital signatures with public key certificates (9 out of 15).

During the last ten years the 3 countries with more publications in this particular area are the USA with 40, UK with 8 and Germany with 7.

4.2. Review for Access control in Healthcare

1453 articles were obtained from the Medline search queries, 234 from the IEEE queries and 200 from the ACM queries. These articles relating to access control in healthcare were reviewed according to their titles and abstracts. From these, 77 full

articles were selected and read. Of these, 59 articles were deemed to be appropriate and were included in the review.

From a total of 27 articles that refer to the system's implementation, 25 were built as prototypes whilst 2 were built in a real life scenario.

From the 34 published articles that mention access control policies, Table 2 shows that 22 refer to the study and analysis of those policies, whilst only 4 of them actually implemented policy based systems as prototypes. In 14 out of these 34 papers, the policies were institutionally or legislatively defined, whilst in only 4 of those 34 articles is it mentioned that end-user can set policies. But none of these 4 policies were actually implemented, not even as prototypes. Further, none of the 34 articles that mention access control policies included the end-users of the system as part of the group that designed and developed those policies.

Finally, 7 articles refer to the need for an override policy definition i.e. an access control system which allows the user to override the current policy in times of emergency, and gain access to patient confidential information that they would not otherwise be able to see.

As for access control models, from the 40 articles that refer the use of access control models, 24 of these mention its study and analysis whilst in 8 articles the models were implemented as prototypes only.

Table 2. No of papers reviewed covering access control policies, models and mechanisms in healthcare between 1996 and 2006.

	1996-99	2000-03	2004-06	Total
Access Control Policy				
Study/Analysis	2	8	12	**22**
Implementation		3	1	**4**
Access Control Model				
Study/Analysis	6	10	8	**24**
Implementation	1	6	1	**8**
Authentication Mechanisms with an implicit access control function				
Study/Analysis	6	10	8	**24**
Implementation	1	6	1	**8**

The most commonly used access control model was RBAC (22 from 40) whilst the most tested authentication mechanism was digital signatures with public key certificates (29 from 41).

Focusing now on the EMR and its users, Table 3 shows the type of information systems that were implemented and in which healthcare institutional setting they were implemented. It also presents the most common types of user groups for those systems.

Table 3. Healthcare institutions, information systems and user groups.

	1996-99	2000-03	2004-06	Total
Healthcare Institution				
Hospital	3	10	7	**20**
Hospital Department		2		**2**
Primary Care		1	1	**2**
Private Care		1	3	**4**
Other		2	5	**7**
Total	**3**	**16**	**16**	**35**
Healthcare Information System				
EPR/EMR/CPR	5	14	15	**34**
Prescription		2	1	**3**
Consultation			1	**1**
Total	**5**	**16**	**17**	**38**
Portal/Internet Access				
Healthcare professionals		1	1	**2**
Patients		1		**1**
Total		**2**	**1**	**3**
User groups				
Medical doctors		2	2	**4**
Nurses		3	2	**5**
Patients		1	4	**5**
Others (HPs,GPs,IT,Pharmacists)	2	13	9	**24**
Total	**2**	**19**	**17**	**38**

Most of the information systems are EMR (34 from 38 articles) and were implemented within hospitals (20 from 35 articles). The end users of the system are mostly healthcare professionals (HPs), general practitioners (GPs), IT and pharmacists. Only in 5 articles is it mentioned that patients might have access to their healthcare information but none of these systems were being used in a real environment.

Table 4 shows the usability problems that were encountered as described in the published articles.

Table 4. Usability problems that were encountered.

Problem type	No of occurrences
Educational Barriers	5
Disruption to workflow & performance	7
Relational Barriers	1
Increase in time for patient session	1
Security concerns	1
Cultural barriers	2
Management problems	4

During the last ten years the 3 countries with more publications in this particular area were the USA with 15, UK with 10 and Greece with 7.

5. Discussion

The main observation from the first two tables was that the results were very similar and access control in healthcare reflects what is happening generally concerning access control in information systems.

Both reviews showed that there is a great interest in defining and studying access control models. However, without a proper access control policy definition, a model cannot be properly implemented and configured, and will never accurately represent both the organization and users' needs in terms of access control. Still, this kind of academic modelling approach works because the vast majority of the models were not implemented in practice. They are analysed as models or, at most, implemented as prototypes. Proper system evaluation is needed before one can conclude that these models are either appropriate or effective.

The preference for using RBAC as the starting point to build an access control model can be explained by the fact that this model allows easier administration and more flexibility in order to be adapted to the workflow and hierarchical needs of a heterogeneous organization.

In terms of authentication mechanisms, the most studied was digital signatures with public key certificates in a Public Key Infrastructure (PKI). Similar results were obtained from both the healthcare domain and the general domain. The use of PKI is extremely complex and usually requires expensive resources, both in terms of manpower expertise and software. At the time the articles under review were written (mostly prior to 2004) PKI systems had not been widely implemented and used in real and complex healthcare scenarios such as public hospitals and other large organizations where resources are usually scarce. After 2004 we could find only one study where PKI was implemented in a real healthcare scenario, but not within an EMR [18]. This study describes a web-based system to access healthcare brain injury information in a regional area. They use digital certificates for authentication. Although this kind of approach deemed to be successful the researchers concluded also that certificates' management is time consuming and requires a strong technical infrastructure and human resources that require continuous monitoring.

Nevertheless, the situation today is changing, although these later developments are not usually reported in research articles. Several national PKI systems have been rolled out, for example, the US Federal PKI system [19], and the Italian identity card system [20], whilst several national healthcare PKI systems now exist e.g. in the UK [21] and Australia [22]. But there is little published research about them.

From this review we found that most healthcare information systems that need access control are EMR systems built within heterogeneous and complex organizations such as hospitals. EMR is becoming more available because its advantages are well acknowledged [13]. However, according to the review, access control policies and models in EMR are usually not implemented and used in real life environments. Some national health services have started to work on such services, e.g. the UK NHS [23], but they are not fully implemented yet.

From those which were implemented within a real setting the end users of the system did not participate in its development and, most of the time did not support its introduction and use [13]. It is also relevant to note that none of the access control systems used within the EMR and in a real environment were being accessed by patients. This situation does not appear to be any better in the national systems that are currently under development, since the patients are not even being informed that their records will be held electronically in these systems, let alone be invited to participate in the design [24]. According to the European legislation [25] patients should be able to access their medical information whenever they request and in an understandable format. Several studies refer to the importance of the benefits to be gained from patients accessing their medical records [26], [27], [28]. However, only one of the analyzed studies [29] provided patients with access to their information, this being via an Internet portal prototype. Again, both healthcare professionals and patients did not participate in the development of this access control system, even though the system focused on patients' access to medical information with the objective of providing for their needs and subsequent healthcare support.

Most access control policies and systems are implemented following legal and institutional requirements. Littlejohns' study [30] shows very clearly the practical problems of implementing information systems within hospitals. According to Littlejohns, the problems arise due to not ensuring that the end users of the system knew why and how the system was being implemented, and for not recognising that education is an extremely important factor to take into account prior to systems' implementation. Further, the complexity of healthcare tasks and processes was underestimated and therefore could not be modelled accordingly. Miller's study [5] analysed the most important barriers to the successful integration of EMR within healthcare practice and found that there were many difficulties with the technology as well as the need for complementary changes and support to be implemented in order to use EMR. These increased the time and costs of implementation while at the same time reduced physicians' use of EMR and consequently the improvement in quality that had been expected. The study also concluded that most physicians needed to spend a great deal of time customizing their electronic forms and had to redesign their workflow processes to use the EMR. Miller et al believe that some of these problems can be reduced with the definition of both public and private policies that can better adapt EMR functionalities, including security, to the needs of its users.

Hackos [31] conclude that the development and implementation of similar projects must start with a realization and understanding of the following: the precise purposes for creating a system; the people who will use the system; what tasks the system will be

used for; and where and how the users will use the system. In this way, users' more specific needs such as workflow processes and activities as well as cultural issues will also be taken into account and modelled.

6. Conclusion

Despite the benefits of EMR, there are some barriers (that may include access control systems) that hinder users from fully taking advantage of them and improving their workflow patterns.

Although access control is a security service that has been widely studied and applied in healthcare systems such as EMR, the fact is that the most interested parties, the users (both healthcare professionals and patients), are not usually consulted when the access control policies are integrated into these systems, and when the system is integrated within their workflow environments. Healthcare professionals usually needed to change their workflow patterns and adapt their tasks and processes in order to use the systems.

We believe that if healthcare professionals and patients support and participate in the access control systems' development process and the access control policy definition then some of problems described above can be minimized ensuring that EMR can be more effectively used in order to provide for better healthcare.

Future work that we propose to undertake includes the development of an access control policy that can incorporate all the stakeholders' needs and views regarding access control (including healthcare professionals and patients) and a further definition of an access control model that can effectively represent these policy rules. We will then proceed with the implementation and evaluation of this access control model within a real healthcare scenario in order to assess whether the improvement in access control systems within EMR, according to the users' needs and workflow patterns, can reduce some of the barriers to the effective use of EMR and therefore provide better healthcare and patient treatment.

References

[1] CERT Coordination Center CMU. CERT/CC Overview Incident and Vulnerability Trends. Carnegie Mellon University; 2003.

[2] Gollman D. Computer Security. 1st ed: John Wiley & Sons; 1999.

[3] Knitz M. HIPPA compliance and electronic medical records: are both possible? . Graduate research report: Bowie State University. Maryland in Europe; 2005.

[4] Sprague L. Electronic health records: How close? How far to go? NHPF Issue Brief. 2004 Sep 29(800):1-17.

[5] Miller RH, Sim I. Physicians' use of electronic medical records: barriers and solutions. Health Aff (Millwood). 2004 Mar-Apr;23(2):116-26.

[6] Becker MY, Sewell P. Cassandra: flexible trust management, applied to electronic health records. 2004; 2004. p. 139-54.

[7] Harris S. CISSP All-in-One Exam Guide. 2nd ed: McGraw-Hill Osborne Media; 2003.

[8] Schneier B. Secrets and Lies: digital security in a networked world: Wiley; 2004.

[9] Blobel B. Authorisation and access control for electronic health record systems. Int J Med Inform. 2004 Mar 31;73(3):251-7.

[10] ISO – International Organization for Standardization. ISO 7498-2: Information processing systems - Open Systems Interconnection - Basic Reference Model - Part 2: Security Architecture. 1989.

[11] Waegemann C. EHR vs. CPR vs. EMR. Healthcare Informatics online. 2003 May 2003.

[12] Cruz-Correia R, Vieira-Marques P, Costa P, Ferreira A, Oliveira-Palhares E, Araújo F, et al. Integration of Hospital data using Agent Technologies – a case study. AICommunications special issue of ECAI. 2005;18(3):191-200.
[13] Institute MR. 7th annual survey of electronic health record trends and usage for 2005. Medical Records Institute. 2005. Medical Records Institute: Medical Records Institute; 2005.
[14] Bakker A. Access to EHR and access control at a moment in the past: a discussion of the need and an exploration of the consequences. Int J Med Inform. 2004 Mar 31;73(3):267-70.
[15] Lehoux P. The Problem of Health Technology: Policy Implications for Modern Health Care. 1st ed: Routledge; 2006.
[16] Knitz M. HIPPA compliance and electronic medical records: are both possible? . Graduate research report: Bowie State University. Maryland in Europe; 2005.
[17] Miller RH, Hillman JM, Given RS. Physician use of IT: results from the Deloitte Research Survey. J Healthc Inf Manag. 2004 Winter;18(1):72-80.
[18] Lemaire E, Deforge D, Marshall S, Curran D. A secure web-based approach for accessing transitional health information for people with traumatic brain injury. Computer Methods and Programmes in Biomedicine. 2006; 213-219.
[19] Alterman P. The US federal PKI and the federal bridge certification authority. Federal PKI steering committee.2005. Available at: http://www.cendi.gov/presentations/alterman_pki_05-13-01.ppt. Acessed on the 20th March 2007.
[20] The Italian electronic identity card. The Italian Ministry of interior. Cybertrust. 2005. Available at: http://www.cybertrust.com/media/case_studies/cybertrust_cs_ital_1.pdf. Accessed on the 20th March 2007.
[21] PKI advaice for Caldicott Guardians & Delegate Authorities. NHS – NSTS phase 2b briefing paper. 2005. Available at: http://www.connectingforhealth.nhs.uk/nsts/docs/pki_advice_caldicott.pdf. Accessed on the 20th March 2007.
[22] Public Key Infrastructure (PKI) Security - About PKI. Australian government – Medicare Australia. 2007 Available at : http://www.medicareaustralia.gov.au/vendors/security_technology/pki_security/about_pki.shtml. Accessed on the 20th March 2007.
[23] Security and access – staff access. NHS – Department of Health. Available at: http://www.nhscarerecords.nhs.uk/nhs/security-and-access/staff-access. Accessed on the 20th March 2007.
[24] The British Medical Association is urging doctors to begin telling their patients about the new electronic health recordKable's Government Computing. 2006 Available at: http://www.kablenet.com/kd.nsf/Frontpage/7A8A73686DE734478025722700554CFC?OpenDocument. Accessed on the 20th March 2007.
[25] Recommandation n° R (97) 5 relative à la Protection des Données Médicales. Comité des Ministres aux États Membres. 1997.
[26] Ross SE, Lin CT. The effects of promoting patient access to medical records: a review. J Am Med Inform Assoc 2003 May-Jun; 10 (3):294.
[27] Honeyman A, Cox B, Fisher B. Potential impacts of patient access to their electronic care records. Inform Prim Care. 2005;13(1):55-60.
[28] Ferreira A, Correia A, Silva A, Corte A, Pinto A, Saavedra A, Pereira A, Pereira AF, Cruz-Correia R, Antunes L. Why facilitate patient access to medical records. Studies in Health Technology and Informatics. 2007. (To be published).
[29] Masys D, Baker D, Butros A, Cowles K. Giving patients access to their medical records via the Internet: The PCASSO experience.
[30] Littlejohns P, Wyatt J, Garvican L. Evaluating computerised health information systems: hard lessons still to be learnt. BMJ. 2003;326:860-3.
[31] Hackos J, Redish J. User and Task Analysis for Interface Design 1st ed: Wiley; 1998.