Handbook of Research on Distributed Medical Informatics and E-Health

Athina A. Lazakidou
University of Peloponnese, Greece

Konstantinos M. Siassiakos
University of Piraeus, Greece

Medical Information Science Reference

MEDICAL INFORMATION SCIENCE REFERENCE

Hershey · New York

Director of Editorial Content: Kristin Klinger
Senior Managing Editor: Jennifer Neidig
Managing Editor: Jamie Snavely
Assistant Managing Editor: Carole Coulson
Typesetter: Chris Hrobak
Cover Design: Lisa Tosheff
Printed at: Yurchak Printing Inc.

Published in the United States of America by
Information Science Reference (an imprint of IGI Global)
701 E. Chocolate Avenue, Suite 200
Hershey PA 17033
Tel: 717-533-8845
Fax: 717-533-8661
E-mail: cust@igi-global.com
Web site: http://www.igi-global.com

and in the United Kingdom by
Information Science Reference (an imprint of IGI Global)
3 Henrietta Street
Covent Garden
London WC2E 8LU
Tel: 44 20 7240 0856
Fax: 44 20 7379 0609
Web site: http://www.eurospanbookstore.com

Copyright © 2009 by IGI Global. All rights reserved. No part of this publication may be reproduced, stored or distributed in any form or by any means, electronic or mechanical, including photocopying, without written permission from the publisher.

Product or company names used in this set are for identification purposes only. Inclusion of the names of the products or companies does not indicate a claim of ownership by IGI Global of the trademark or registered trademark.

Library of Congress Cataloging-in-Publication Data

Handbook of research on distributed medical informatics and e-health / Athina A. Lazakidou and Konstantinos M. Siassiakos, editors.

p. ; cm.

Includes bibliographical references and index.

Summary: "This book provides a compendium of terms, definitions and explanations of concepts, processes and acronyms related to different areas, issues and trends in Distributed Medical Informatics, E-Health and M-Health"--Provided by publisher.

ISBN 978-1-60566-002-8 (h/c)

1. Medical telematics--Handbooks, manuals, etc. I. Lazakidou, Athina A., 1975- II. Siassiakos, Konstantinos M.

[DNLM: 1. Telemedicine--methods. 2. Medical Informatics Applications. W 83.1 H236 2009]

R119.95.H36 2009

610.285--dc22

2008014431

British Cataloguing in Publication Data
A Cataloguing in Publication record for this book is available from the British Library.

All work contributed to this book set is original material. The views expressed in this book are those of the authors, but not necessarily of the publisher.

If a library purchased a print copy of this publication, please go to http://www.igi-global.com/agreement for information on activating the library's complimentary electronic access to this publication.

Chapter III
Security of Electronic Medical Records

Ana Ferreira
University of Kent, UK & University of Porto, Portugal

Ricardo Cruz-Correia
CINTESIS, Portugal & University of Porto, Portugal

Luís Antunes
LIACC, University of Porto, Portugal

David Chadwick
University of Kent, UK

ABSTRACT

This chapter reports the authors' experiences regarding security of the electronic medical record (EMR). Although the EMR objectives are to support shared care and healthcare professionals' workflow, there are some barriers that prevent its successful use. These barriers comprise not only costs, regarding resources and time, but also patient / health professional relations, ICT (information and communication technologies) education as well as security issues. It is very difficult to evaluate EMR systems; however some studies already made show problems regarding usability and proper healthcare workflow modeling. Legislation to guide the protection of health information systems is also very difficult to implement in practice. This chapter shows that access control, as a part of an EMR, can be a key to minimize some of its barriers, if the means to design, develop and evaluate access control are closer to users' needs and workflow complexity.

Copyright © 2009, IGI Global, distributing in print or electronic forms without written permission of IGI Global is prohibited.

INTRODUCTION

Healthcare is information and knowledge driven. Good healthcare depends on taking decisions at the right time and place, according to the right patient data and applicable knowledge (Friedman C and Wyatt J, 2006). Communication is of most relevance in today's healthcare settings, as health related activities, such as delivery of care, research and management, depend on information sharing and teamwork (Coiera, 2003).

Providing high-quality health care services is an information-dependent process. Indeed, the practice of medicine has been described as being dominated by how well information is processed or reprocessed, retrieved, and communicated (Barnett, 1990). An estimated 35 to 39 percent of total hospital operating costs has been associated with patient and professional communication activities (Richart, 1970). Physicians spend over a quarter (Commission, 1995, Mamlin and Baker, 1973) and nurses half (Korpman and Lincoln, 1998) of their time writing up patients' charts.

Patient records exist to memorize and communicate the data regarding a particular individual and to help deliver care to him or her. Records are not only an information system but also a communication system, to enable communication between different health professionals and between the past and present (Dick and Steen, 1997, Nygren et al., 1998). Patient records, the patient and published evidence are the three sources needed for the practice of evidence-based medicine (Friedman C and Wyatt J, 2006).

After decades of development of information systems, designed primarily for physicians and other healthcare managers and professionals, there is an increasing interest in reaching consumers and patients directly through computers and telecommunication systems (Chuva Mt et al., 2006). Consumer health informatics is designed to empower consumers by putting health information into their hands, including information on their own health, such as diagnoses, lab results, personal risk factors and prescribed drugs. All this information requires strong security means.

Information security is usually defined by three main characteristics (Cen/Tc251), (Harris S, 2003): 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: the complexity of the security technology itself; the difficulty of classifying the information that is to be protected; and the use of the technology by humans (usually the most problematic factor (Schneier B, 2004)). 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.

LEGISLATION

The Health Insurance Portability and Accountability Act (HIPAA) of 1996 (USA Congress, 1996) is the American legislation that provides for the security and privacy as well as health insurance for American workers and their families. Title I of HIPAA protects health insurance coverage for workers and their families when they change or lose their jobs. Title II of HIPAA, the Administrative Simplification (AS) provisions, requires the establishment of national standards for electronic

health care transactions and national identifiers for providers, health insurance plans, and employers. The AS provisions also address the security and privacy of health data. The standards are meant to improve the efficiency and effectiveness of the nation's health care system by encouraging the widespread use of electronic data interchange in the US health care system. Despite all this defined legislation, and no matter the status of IT or financial resources, compliance with HIPAA and functional implementation of EMR systems requires a change in the culture of an organization (Knitz M, 2005).

The European experience on the same matters is described in a 1997 recommendation (Ministers Committee, 1997) from the European Community that established to all its members a set of principles and recommendations regarding the protection of medical data. From these we highlight the following security recommendations:

9.2: In order to ensure in particular the confidentiality, integrity and accuracy of processed data, as well as the protection of patients, appropriate measures should be taken:

e: with a view to selective **access to data** and the security of the medical data, to ensure that the processing as a general rule is so designed as to enable the separation of: identifiers and data relating to the identity of persons; administrative data; medical data; social data; genetic data

In 2004 the European Community (Ministers Committee, 2004) made some more recommendations on the impact of information technologies on health care – the patient and Internet.

As an example, in October 1998 Portugal adopted all these recommendations (law 67/98 — Personal Data Protection, and later law 12/2005 on Personal Genetic Health Information). It is, however, interesting to present the summary of two studies made in Portugal on this subject. The first one was made by the Portuguese National Data Protection Commission (CNPD) in 2004, and is a report on the health information processing status of most Portuguese Hospitals; the second is a study made by some medical students at Hospital de São João, Porto, regarding the opinions of medical doctors about access control, further described in the Access Control Section within this chapter (Pinho C et al., 2006).

Regarding the CNPD report we highlight the following conclusions: (note that this study was made in 2004 and since then some anomalies are bound to have been corrected):

- The CNPD was not notified, as is mandatory by law, in 50% of the cases where health information is processed.
- Patients where not informed when their data was used for research purposes.
- In 35% of the applications, there was not a logical separation between health information and administrative data.
- Regarding passwords, 172 applications had it whilst 12 did not. The most commonly used password is the users' name.
- In 136 applications only 2 followed the conservation time enforced by the CNPD.
- Regarding the health information that was kept in paper, confidentiality was not a concern. Requests and information travel through the hospital without any kind of protection.

Furthermore, the European Union's data protection directive (in effect since October 1998) requires all member countries to enact legislation enabling patients to have access to their medical records (Eysenbach, 2000). This Recommendation (Ministers Committee, 1997) also defines that patients should be able to access their clinical information whenever they request and have means to control who can see and change that information. However, this is still not common practice mostly because of logistic and also cul-

tural issues. The general idea is that healthcare professionals think that patient's access to their medical records may negatively affect their relationship with the patients. Patients themselves do not know if they want to see their medical record and if they do, will it be helpful and will they understand it anyway.

There are however some studies that show that patients' access to their medical records brings more benefits than not, and so the authors believe this is prone to become more common in the years to come (Ferreira A et al., 2007a).

EMR INTEGRATION AND SECURITY

The introduction of the EMR within healthcare organizations depends on integrating heterogeneous information that is usually scattered over different locations (Waegemann C, 2003, Cruz-Correia R et al., 2005). 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 (Institute, 2005). This and the distributed nature of the information stress the need for security requirements to be taken seriously (Bakker A, 2004). In healthcare organisations that require intra and inter-organizational interactions, authorisation and access control mechanisms cannot only be organized at a user level, but need also to be defined at other levels that can reflect those dynamic interactions. To do this, a series of structured and formal policies, models and roles must be defined (Blobel, 2004).

Although standardization and data exchangeability are topics that receive global attention, many of the healthcare applications are highly dedicated and specific to the environment in which they are used. Their functions range from pure administrative and billing to the creation of research databases, decision support, picture archiving, and image analysis.

Experience has shown that physicians are horizontal users of information technology (Greenes and Shortliffe, 1990). Rather than becoming power users of a narrowly defined software package, they tend to seek broad functionality across a wide variety of systems and resources. Thus, routine use of computers, and of EMR, will be most easily achieved if the computing environment offers a critical mass of functionality that makes the system both smoothly integrated and useful for essentially every patient encounter. Also, many computer applications today use information from several data sources.

With the introduction of networked systems within our healthcare organizations, there are new opportunities to integrate a wide variety of resources through single clinical workstations. In such an environment, diverse clinical, financial, and administrative databases need to be accessed and integrated, typically by using both networks to tie them together and a variety of standards for sharing data among them. Thus the clinical data repository has developed as an increasingly common idea.

Patient data quality in computer-based patient records has been found to be rather low in several health information systems (Hogan and Wagner, 1997, Hammond et al., 2003, Hohnloser et al., 1994). Furthermore, the assessment of the correctness of collected patient data is a difficult process even when we are familiar with the system in which it was collected (Berner and Moss, 2005). Therefore, one of the main challenges of health information systems or networks is to be able to gather the different parts of the medical record of a patient without any risk to mix them with those of another patient (Quantin et al., 2004, Arellano and Weber, 1998). Erroneous patient identification has also an impact on hospital charging, as subsidiary partners refuse to pay for misidentified medical procedures.

In May 2003, the Department of Biostatistics and Medical Informatics implemented a virtual electronic patient record (Cruz-Correia et al.,

2005) for the Hospital S. João (HSJ), a university hospital with over 1350 beds. The system integrates clinical data from 10 legacy hospital departments information systems (HDIS) and the diagnosis related groups (DRG) and hospital administrative databases (HAD), aiming to deliver the maximum information possible to health professionals. Over 800 medical doctors use the system on a daily basis and the HSJ-VEPR retrieves an average of 3000 new reports each day (in PDF or HTML formats).

To detect and prevent possible problems in the HSJ-VEPR, Nagios (Koffler and Galstad, 2002) version 2 (a system and network monitoring application) was installed and configured (Cruz-Correia et al., 2006). Sometimes a HDIS sends an abnormal number per day (either too big or to small) of reports to HSJ-VEPR. This normally reflects some kind of HDIS problem. It was decided to develop a dynamic system that learns from the number of reports received previously in the same weekday and implement it as a Nagios plug-in. To define an initial knowledge base, a table was created where each record included the number of reports of a particular HDIS in a particular week day (Table 1). The system calculates percentile 2.5 and 97.5 to be used as lower and higher margins of the normality interval.

The comparison of current and previous IS behavior allows the detection of irregularities. In this case the knowledge used to trigger alerts is build from past experience. We feel that as the time goes, we will have more records and consequently the percentiles for normality the range can be changed from [2.5, 97.5] to [1, 99] increasing even more the method specificity.

Table 1. Percentiles 2.5 and 97.5 of reports sent in 2005 by a particular HDIS

Percentile	Mon.	Tue.	Wed.	Thu.	Fri.	Sat.	Sun.
2.5	82	100	148	121	99	45	40
97.5	561	595	560	674	668	300	364

One of the main challenges of health information systems integration is to gather parts of the medical record without jeopardizing patient data quality. The HSJ-VEPR indexes all information to a unique hospital patient number. Identification problems occur when the hospital patient number or the hospital encounter number that are being sent by the HDIS are wrong (Cruz-Correia R et al., 2006). These errors could lead to associating the report to a different patient.

The idea of detecting identification errors is based on checking the name and date of birth sent by the HDIS against the hospital administrative database (HAD). The main difficulty arises from small changes in patient names, which would originate false identification errors (e.g.: "Jessica Maria Smith Murphy" <=> "Jessica Maria S. Murphy").

The patient data quality algorithm is triggered with the arrival of a new clinical report from a particular HDIS, and is divided in three phases: 1st detect errors in hospital patient number, 2nd detect errors in hospital encounter numbers and 3rd store report in HSJ-VEPR .

When errors occur, a report is generated and sent to the HDIS administrators. This report includes a description of the error along with all information sent by HDIS and retrieved from HAD. By doing so, the origin of the error can be traced and corrected.

This module has been deployed in July 2005, and is being configured for each HDIS. Currently it scans an average of 65.000 reports per month (2.100 per day). In the first 6 months 423 patient identification errors were found within 391.258 reports checked.

The detection of these errors has triggered both their correction on each HDIS as well as a change on department workflow which resulted in less identification errors. Two errors where also found on HAD, caused by inappropriate re-utilization of a unique hospital patient number.

Cross-checking between integrated distributed systems may be used to guarantee global

patient data quality and integrity. As proper checking methods are put in place, the number of inconsistencies in integrated systems tends to decrease as people awareness of these silent problems increases.

As stated in (Institute, 2005) the main factor that is driving the need for EMR systems to be implemented is the need to improve clinical processes or workflow efficiency. Also, as stated in (Lehoux P, 2006), information technologies are used in healthcare to record, transmit and provide access to administrative and clinical information, so this should imply that access to and use of information respects confidentiality and brings efficiency and quality to healthcare. For now, the reality is that EMRs still do not integrate easily among healthcare professionals' daily workflow (Miller R. H and Sim I, 2004) in order to be efficiently used.

One obstacle mentioned by healthcare professionals for the use and integration of EMR within healthcare is patient privacy (Knitz M, 2005). As stated above, in order to protect patients' privacy it is essential to at least provide for information confidentiality. When asked, healthcare professionals say they think EMR have problems in terms of security due to its ease of distribution and wider online access (Miller R. H et al., 2004).

There are also other barriers that impede the effective integration of EMR within the healthcare practice. These barriers can be grouped in: time/cost, relational and educational (Sprague L, 2004, Miller R. H and Sim I, 2004). Apart from the cost of EMR integration and the time healthcare professionals spend using the system in order to access and insert information there are other issues that relate more with human processes and their daily tasks. These are the relational and educational barriers explained below.

The relational barrier includes the perceptions that the physician and the patient have about the use of the EMR and how their relationship may be affected by it. As an example, when the physician uses the computer during a consultation, the patient may be uncomfortable with the lack of attention given to him and have doubts about the information being written.

The educational barrier comprises the lack of proficiency and difficulties that healthcare professionals have in interacting with the EMR in order to perform their daily tasks (Becker and Sewell, 2004). Because healthcare professionals do not participate in the design and development of working tools (in this case the EMR), they usually have to redesign their practice workflow and processes, which is very challenging and consumes more time and costs (Miller R. H and Sim I, 2004). In order to facilitate their daily workflow, since they access and use the EMR, the users must be involved in its design and development as they were within the case study described above in the HSJ (Ferreira A et al., 2005).

Although there is usually an initial plan describing the rules to access an EMR, devised by engineers, promoters and implementers, its access in practice is often different from what was envisaged and decided at first (Kling R, 1991, Lehoux P et al., 1999). Users may have to reorganize their tasks and routines to accommodate the system; or they may even circumvent the rules that have been established for accessing the system (Lehoux P et al., 1999, Akrich M, 1994) because they were too cumbersome or time-consuming or both (e.g. by sliding in a personal ID card and keying in a password).

An EMR should focus on helping and facilitating users to follow their daily processes without much effort and time. It should improve the working life of the health care professionals and bring benefits to them and their patients, rather than imposing costs on them, in terms of time and effort, with no perceivable benefits to either them or their patients. Therefore new security models and technologies to be implemented should focus on human processes and needs rather than on theoretical studies.

INFORMATION SYSTEMS EVALUATION

Many of the problems presented previously could be avoided if proper systems' evaluation could be provided and means to redesign and improve the system were easy to apply. This evaluation should be done, ideally, before, during and after information system's development and installation. How do we know if a system is really working and performing the way it is supposed to? How can we know how to improve and better adapt that system either because the circumstances or the objectives changed? The answer is, of course: evaluation.

The developing and good design of usable technology is very important as these can make users more productive and comfortable when using the system. Once more, the emphasis is usually on technology and not on users when systems are developed. Developers do not usually understand users, their tasks, workflow and environment. A system interface is the bridge between both the world of technology and the world of the user, the means by which the user interact with the system (Hackos Joann and Redish Janice, 1998). What can be more important than making sure people use the system in their natural physical, social and cultural environment?

For example in (Brostoff et al., 2005) usability and design methods were used to evaluate a specific software tool. Questionnaires were also applied to achieve a more generic feeling for the tool. According to their results, this evaluation and interface redesign improved its efficiency, making the tool easier to use and understand.

Another example is briefly described in (Hackos Joann and Redish Janice, 1998) where programmers designing a medical records' system completely changed their initial software interface after they visited the site. They discovered that the workflow among departments and individuals proceeded in a different manner to what they had imagined. They watched people performing their tasks and interviewed medical records' staff about the nature of their work. The message then is to design from reality and not from assumptions. In conclusion, evaluation methods must focus on users' behaviour as well as attitudes and opinions.

However, healthcare information systems' evaluation is not trivial (Friedman C and Wyatt J, 2006). Medical informatics is a combination of domains that makes any evaluation very complex and never definitive. There is not a specific method for all cases and one of the most important things to take into account is to choose the right method at the right moment in time. The following section presents a review about IS evaluation.

The authors performed a brief review about evaluation methods used for information systems (IS), most of them in healthcare. This review

Table 2. Results for the review on IS evaluation

Objectives	Total
Presents methods to evaluate information systems	13
Evaluate evaluation methods	10
Improve technologies or applications	
Information System's Evaluation	4
Methods of evaluation	
Others	6
Usability	4
Questionnaires/interviews	4
Literature review	3
Not mentioned	3
Cognitive science	2
Quantitative/qualitative	2
Soft-systems	2
Heuristics	2
Ergonomic methods and tools	1
Problems encountered	
No proper evaluation methods	12
Applications are difficult to use	6
Complex workflow analysis and decisions	5
Costs and insufficient policies	2
Insufficient infrastructure	1

comprised 27 articles about this subject from 1999 till 2006, 3 of which are websites. Some of the articles described new evaluation methods, others the results and application of some methods and yet others the evaluation of the methods themselves.

The main results of this review are presented in Table 2.

In a similar proportion, the reviewed articles either try to introduce new methods of evaluation or the result of analyzing some existing evaluation methods. There is a split worry in order to find the most adequate evaluation methods as well as trying to check what the main problems are with the existing ones.

The most common used methods to evaluate IS, besides proprietary ones, are usability methods, questionnaires or interviews.

The most frequent problems encountered within the articles reviewed regarding evaluation methods are that these are usually not right for the evaluation that needs to be performed. Also, regarding the IS that were evaluated, the results show that the problems of the evaluated applications are not, as was probably expected, the costs that these applications incur. Results of evaluation show that applications are often difficult to use and that workflow and decisions that those applications are supposed to help are usually too complex and cannot be implemented.

There are many issues regarding IS evaluation and this is becoming very challenging as still no adequate methods can be used in a generic fashion. The problems encountered are recurrent. They deal with the fact that IS are not developed according to users' needs, workflow tasks and complexity. This justifies why it is so difficult to choose or develop the right evaluation methods for IS. There seems to be a problem from conception and not on the evaluation side. This makes it hard to decide which methods to choose and apply, and first of all, what is needed to evaluate in first place.

If it is so hard to do this within the IS, it is harder to do this within parts of the IS as is for example security, and more specifically access control.

ACCESS CONTROL

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).

Access control is conceptually part of the authorisation process that checks if a user can access the resources he requested.

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 (Blobel, 2004). 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) (ISO, 1989). 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 and user needs 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.

We are including all three steps to access an IS within the scope of the review presented in this section 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.

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) in general and applied to the healthcare environment (Ferreira A et al., 2007b). Searches were made in medical databases such as Medline (that included the BMJ-British Medical Journal) as well as IEEE Xplore and ACM.

As can be seen in Table 3, 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

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.

With the healthcare articles, 59 were deemed to be appropriate and were included in the review. From a total of 27 articles that refer to the system's

Table 3. Number 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**

Table 4. Number 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**

Table 5. 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**

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 6 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 (Ferreira A et al., 2006). 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.

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 5 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.

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. 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.

Table 6. Problems regarding EMR integration encountered in the revised articles

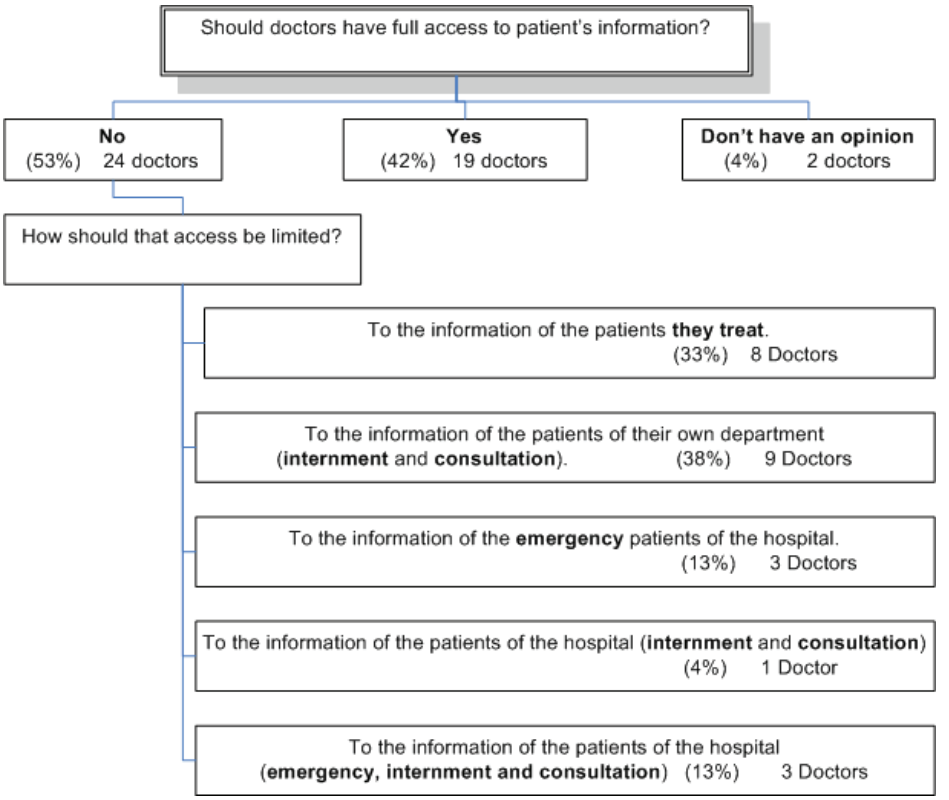
Problem type	Number of occurrences
Disruption to workflow & performance	7
Educational Barriers	5
Management problems	4
Cultural barriers	2
Security concerns	1
Relational Barriers	1
Increase in time for patient session	1

Table 6 shows the usability problems that were encountered as described in the published articles. Not surprisingly, most of them relate mainly with the disruption of workflow and performance when the EMR is used as well as with educational problems.

As an example, in order to find out more about end users' opinion on access control to EMR, this study (Pinho C et al., 2006) applied a survey to medical doctors within a university hospital. Most respondents agree that access control levels must exist for EMR and that not all doctors must have total access to all patient records. They indicate that more sensitive information (e.g. HIV) must only be accessed by doctors that treat those patients.

A great number of doctors also revealed that patients should not have total access to their own medical records (Figure 1). This must be further analysed as patients should have the right to access all their medical information, if they require. It is surprising that most doctors think they can access all the information about a patient they are treating and, at the same time, feel the patients themselves cannot have the same right regarding their own information.

Figure 1. Doctors' response regarding full access to patients' records



Further, most doctors thought that nurses should not access all patient information (Figure 2). But how different would these results be if the same questionnaire was applied to the nurses or other category of healthcare professionals?

As a reflection of this specific study, the authors' experience within this field by having contact with both healthcare and IT professionals in various lectures and workshops shows that healthcare professionals have great difficulty in defining the best policies to control the access to IS.

Although there is legislation and healthcare professionals know the way they perform their daily tasks, it is quite hard for them to define accurately, the correct access rights to an IS. Nevertheless, healthcare professionals feel that their participation is essential in order to adapt access control policies to their needs.

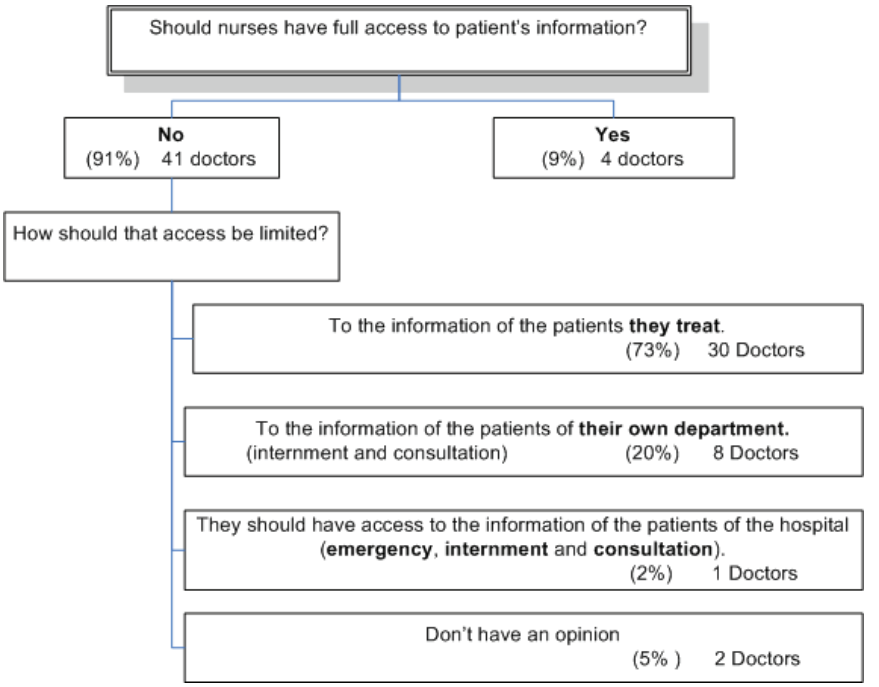
They further agree that access control needs to be defined by a multidisciplinary team, including themselves, and reach a consensus to the best of their ability. Only this way can access control and the right usage of EMR be achieved.

DISCUSSION

EMR are essential to today's shared care and although security is very difficult to achieve it is regarded as having a fundamental role to play.

An EMR should focus on facilitating users to follow their daily processes without much effort and time. These processes must be taken into account when new security models and technologies are implemented. Further, automatic verification of data quality must be provided and used to trigger alerts of malfunctions and inconsistencies, ensuring data integrity and better health care.

Figure 2. Doctor responses regarding nurses' full access to patients' records



Apart from security, IS evaluation is an essential requirement to build proper and efficient IS. However, this is very challenging as still no adequate methods can be used in a generic fashion. Some evaluations that are made encounter problems that deal mainly with the fact that IS are not developed according to users' needs, workflow tasks and complexity. This justifies why it is so difficult to choose or develop the right evaluation methods for IS. There seems to be a problem from conception and not on the evaluation side. This makes it hard to decide which methods to choose and apply, and first of all, what is needed to evaluate.

Regarding access control, although there is legislation and healthcare professionals know the way they perform their daily tasks, it is quite hard for them to define accurately, the correct access rights to an IS. From legislation to practice, the development of access control (as well as other healthcare IS such as EMR) has several problems. Nevertheless, healthcare professionals feel that their participation is essential in order to adapt access control policies to their needs. They further agree that access control needs to be defined by a multidisciplinary team, including themselves, and reach a consensus to the best of their ability.

CONCLUSION

It is a fact that the end users of a product seldom participate in its design and definition although everybody agrees that this would probably save a lot of costs and time. In healthcare, these problems go further and interfere with the appropriate use of the EMR, its security and furthermore, with the provision of proper patient healthcare.

The authors believe that if healthcare professionals and patients support and participate in the access control systems' design and development process, more specifically the access control policy definition that defines and links security from legislation to practice, then some of the

problems regarding EMR integration and use that were described within this chapter could be minimized.

REFERENCES

Akrich M. (1994). Comment sortir de la dichotomie technique/société : Presentation des diverses sociologies de la technique. De la préhistoire aux missiles balistiques : De líntelligence sociale des techniques. *La Découverte Latour & Lemonnier***,** 105-131.

Arellano, M. G.,Weber, G. I.. (1998). Issues in identification and linkage of patient records across an integrated delivery system. *J Healthc Inf Manag, (12)***,** 43-52.

Bakker A. (2004). 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, (73)***,** 267-70.

Barnett, O. (1990). Computers in medicine. *JAMA, (263)***,** 2631-2633.

Becker, M. Y.,Sewell, P. (2004). Cassandra: flexible trust management, applied to electronic health records.

Berner, E.,Moss, J. (2005). Informatics Challenges for the Impending Patient Information Explosion. *J Am Med Inform Assoc,* 12**,** 614-7.

Blobel, B. (2004). Authorisation and access control for electronic health record systems. *Int J Med Inform,* 73**,** 251-7.

Brostoff, S., Sasse, M. A., Chadwick, D., Cunningham, J., Mbanaso, U.,Otenko, S. (2005). "R-What?" Development of a role-based access control (RBAC) policy-writing tool for e-scientists. *Software - Practice and Experience, (38)***,** 835-856.

CEN/TC251 (1999). ENV 12251: Health Informatics - Secure user identification for health care management and security of authentication by passwords. *European Standards in Health Informatics.* CEN.

Chuva MT, Fernandes MT, Correia C, Barbosa L, Silva MJ, Gomes MJ, Moreira MM, Gomes MM, Vinhas MS, Dias M, Moreira M,Ferreira A. (2006). Attitudes and opinions of patients and healthcare professionals about the use of coomputers in primary care – systematic review. *IX Jornadas Científicas dos Estudantes de Medicina. Faculdade de Medicina da Universidade do Porto.*

Coiera, E. (2003). *Guide to health informatics*, Arnold.

Commission, A. (1995). For your information: a study of information management and systems in the acute hospital.

Cruz-Correia R, Vieira-Marques P, Costa P, Ferreira A, Oliveira-Palhares E, Araújo F,Costa-Pereira A. (2005). Integration of Hospital data using Agent Technologies – a case study. *AICommunications special issue of ECAI, (18)***,** 191-200.

Cruz-Correia R, Vieira-Marques P, Ferreira A, Oliveira-Palhares E, Costa P,Costa-Pereira A. (2006). Monitoring the integration of hospital information systems: how it may ensure and improve the quality of data. *Stud Health Technol Inform (121)***,** 176-182.

Cruz-Correia, R., Vieira-Marques, P., Costa, P., Ferreira, A., Oliveira-Palhares, E., Araujo, F.,Costa-Pereira, A. (2005). Integration of hospital data using agent technologies - a case study. *AI Communications, (18)***,** 191-200.

Cruz-Correia, R., Vieira-Marques, P., Ferreira, A., Oliveira-Palhares, E., Costa, P.,Costa-Pereira, A., 2006. Monitoring the integration of hospital information systems: how it may ensure and improve the quality of data. *Stud Health Technol Inform, (121)***,** 176-182.

Dick, R.,Steen, E., 1997. *The Computer-based patient record: An essential technology for healthCare*.

Eysenbach, G. (2000). *Consumer health informatics. BMJ, (320)*, 1713-16.

Ferreira A, Correia A, Silva A, Corte A, Pinto A, Saavedra A, Pereira A, Pereira AF, Cruz-Correia R,Antunes L. (2007a). Why facilitate patient access to medical records. *Studies in Health Technology and Informatics, (127)*, 77-90.

Ferreira A, Cruz-Correia R, Antunes L,Chadwick D W. (2007b). Access Control: how can it improve patients' healthcare? *Studies in Health Technology and Informatics, (127)*, 65-76.

Ferreira A, Cruz-Correia R, Antunes L, Farinha P, Oliveira-Palhares E, Chadwick D. W,Costa-Pereira A. (2006). How to Break Access Control in a Controlled Manner. *CBMS2006*. Salt Lake City, USA.

Ferreira A, Cruz-Correia R, Antunes L, Oliveira-Palhares E, Farinha P,Costa-Pereira A. (2005). How to start modelling access control in a healthcare organization. *10th International Symposium for Health Information Management Research*. Greece.

Friedman C,Wyatt J. (2006). *Evaluation methods in biomedical informatics*, Springer.

Greenes, R.,Shortliffe, E. (1990). Medical Informatics: an emerging academic discipline and institutional priority. *JAMIA, (263)*, 1114-20.

Hackos JoAnn,Redish Janice. (1998). *User and task analysis for interface design* Wiley.

Hammond, K., Helbig, S., Benson, C.,BM, B.-S. (2003). Are electronic medical records trustworthy? Observations on copying, pasting and duplication. *AMIA Annual Symposium*.

Harris S, 2003. *CISSP All-in-one exam guide*. McGraw-Hill Osborne Media.

Hogan, W.,Wagner, M. (1997). Accuracy of data in computer-based patient records. *J Am Med Inform Assoc, (4)*, 342-355.

Hohnloser, J., Fischer, M., Konig, A.,Emmerich, B. (1994). Data quality in computerized patient records. Analysis of a haematology biopsy report database. *Int J Clin Monit Comput, (11)*, 233-40.

Institute, M. R., 2005. 7th annual survey of electronic health record trends and usage for 2005, Medical records institute. (2005). *Medical records institute, medical records institute*.

Kling R, 1991. Computerization and social transformations. Science, technology and human values. *Science, Technology and Human Values, (16)*, 342-267.

Knitz M. (2005). *HIPPA compliance and electronic medical records: are both possible?* . Bowie State University: Maryland, Europe.

Koffler, D.,Galstad, E. (2002). *Nagios 1.x documentation*.

Korpman, R.,Lincoln, T. (1998). The computer-stored medical record: For whom ? *J Am Med Inform Assoc, (259)*, 3454-3456.

Lehoux P, 2006. *The Problem of Health Technology: Policy Implications for Modern Health Care*, Routledge.

Lehoux P, Sicotte C,Denis J. (1999). Assessment of a computerized medical record system: disclosing its scripts of use. *Evaluation and Program Planning, (22)*, 439-453.

Mamlin, J.,Baker, D., 1973. Combined time-motion and work sampling study in a general medicine clinic. *Medical Care, (11)*, 449-456.

Miller R. H, Hillman J. M,Given R. S, 2004. Physician use of IT: results from the Deloitte Research Survey. *J Healthc Inf Manag, (18)*, 72-80.

Miller R. H,Sim I, 2004. Physicians' use of electronic medical records: barriers and solutions. *Health Aff (Millwood), (23)*, 116-26.

Ministers Committee (1997). Recommendation No. R (97) 5 of the Committee of Ministers to Member States on the Protection of Medical Data. IN Europe, C. o. (Ed.).

Ministers Committee (2004). Recommendation Rec(2004)17 of the Committee of Ministers to member states on the impact of information technologies on health care – the patient and Internet IN Europe, C. o. (Ed.).

Nygren, E., Wyatt, J. C.,Wright, P. (1998). Helping clinicians to find data and avoid delays. *Lancet, (352)*, 1462-6.

Pinho C, Sá C, Mendes E, Santos E, Silva F, Sousa F, Gomes F, Abreu F, Mota F, Aguiar F, Faria F, Macedo F,Martins S. (2006). Electronic patient records - who should access what? Doctors' view. *Biostatistics and Medical Informatics Department - Faculty of Medicine of Porto.*

Quantin, C., Binquet, C., Bourquard, K., Pattisina, R., Gouyon-Cornet, B., Ferdynus, C., Gouyon, J. B.,Allaert, F. A., 2004. A peculiar aspect of patients' safety: the discriminating power of identifiers for record linkage. *Stud Health Technol Inform, (103)*, 400-6.

Richart, R., 1970. Evaluation of a medical data system. *Computers and Biomedical Research, (3)*, 415-425.

Schneier B, 2004. *Secrets and Lies: digital security in a networked world*, Wiley.

Sprague L, 2004. Electronic health records: How close? How far to go? *NHPF Issue Brief*, 1-17.

USA Congress, 1996. HIPAA - Health Insurance Portability and Accountability Act IN Government, U. (Ed.), Public Law (pp. 104-191) 104th Congress.

Waegemann C, 2003. EHR vs. CPR vs. EMR. *Healthcare Informatics online*.

KEY TERMS

Access Control: Set of security features that control how users and systems communicate and interact with other systems and resources. They protect systems and resources from unauthorized access and can be a component that participates in defining the level of authorisation after an authentication is successful. Access control is extremely important because is one of the 1st lines of defence used to fight against unauthorized access to systems and network resources. *Shon Harris, CISSP. All in one CISSP Certification. MCGrawHill, Osbourne, 2003.*

EMR: Electronic medical record (EMR) is a medical record in digital format. A Medical record is a systematic documentation of a patient's medical history and care. The term 'Medical record' is used both for the physical folder for each individual patient and for the body of information which comprises the total of each patient's health history. Although medical records are traditionally compiled and stored by health care providers, personal health records maintained by individual patients have become more popular in recent years.

Information Security: Is the process of protecting data from unauthorized access, use, disclosure, destruction, modification, or disruption. This means protecting the confidentiality, integrity and availability of data regardless of the form the data may take: electronic, print, or other forms.

IS: An information system (IS) is a system, automated or manual, that comprises people, machines, and/or methods organized to collect, process, transmit and disseminate data that represent user information.

Medical Informatics: The rapidly developing scientific field that deals with biomedical information, data, and knowledge - their storage, retrieval, and optimal use for problem solving and decision making. The emergence of this new discipline has been attributed to "advances in computing and communications technology, to an increasing awareness that the knowledge base of medicine is essentially unmanageable by traditional paper-based methods, and to a growing conviction that the process of informed decision making is as important to modern biomedicine as is the collection of facts on which clinical decisions or research plans are made." *Edward Shortliffe, M.D., Ph.D. What is medical informatics? Stanford University, 1995.*