Certification and Security in Health-Related Web Applications:
Concepts and Solutions

Anargyros Chryssanthou
Hellenic Data Protection Authority, Greece

Ioannis Apostolakis
National School of Public Health, Greece

Iraklis Varlamis
Harokopio University of Athens, Greece

Medical Information Science Reference

MEDICAL INFORMATION SCIENCE REFERENCE

Hershey · New York

Director of Editorial Content: Kristin Klinger
Director of Book Publications: Julia Mosemann
Acquisitions Editor: Lindsay Johnston
Development Editor: Dave DeRicco
Publishing Assistant: Milan Vracarich Jr.
Typesetter: Michael Brehm
Production Editor: Jamie Snavely
Cover Design: Lisa Tosheff

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

Library of Congress Cataloging-in-Publication Data

Certification and security in health-related web applications : concepts and solutions / Anargyros Chryssanthou, Ioannis Apostolakis and Iraklis Varlamis, editors.
p. cm.
Includes bibliographical references and index.
Summary: "This book aims to bridge the worlds of healthcare and information technology, increase the security awareness of professionals, students and users and highlight the recent advances in certification and security in health-related Web applications"--Provided by publisher.
ISBN 978-1-61692-895-7 (hardcover) -- ISBN 978-1-61692-897-1 (ebook) 1. Medical informatics--Security measures. 2. Medicine--Databases--Security measures. 3. Medicine--Databases--Certification. 4. Internet in medicine--Security measures. I. Chryssanthou, Anargyros, 1979- II. Apostolakis, Ioannis, 1961- III. Varlamis, Iraklis, 1974-
R859.7.S43C47 2011
610.285--dc22
2010016324

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

Chapter 13
Password Sharing and How to Reduce It

Ana Ferreira
Cintesis, Portugal & University of Kent, UK

Ricardo Correia
Cintesis, Portugal

David W Chadwick
University of Kent, UK

Henrique Santos
University of Minho, Portugal

Rui Gomes
Hospital Prof. Doutor Fernando Fonseca, Portugal

Diogo Reis
Hospital S. Sebastião, Portugal

Luis Antunes
Instituto de Telecomunicações, Portugal

ABSTRACT

Password sharing is a common security problem. Some application domains are more exposed than others and, by dealing with very sensitive information, the healthcare domain is definitely not exempt from this problem. This chapter presents a case study of a cross section of how healthcare professionals actually deal with password authentication in typical real world scenarios. It then compares the professionals' actual practice with what they feel about password sharing and what are the most frequent problems associated with it. Further, this chapter discusses and suggests how to solve or minimize some of these problems using both technological and social cultural mechanisms.

DOI: 10.4018/978-1-61692-895-7.ch013

INTRODUCTION

Health care is an industry sector considered to be exposed to high risks regarding information security. Nevertheless, today's technology and good practices provide a range of controls to mitigate (up to a certain level) most of those risks, especially those related to electronic health records. The biggest risk faced is a lack of understanding of the complex environments that our health services present and ensuring that users understand and comply with local policies. Convergence towards a viable universal solution is not imminent. Therefore trust in e-health is decidedly more fragile as compared with many other industry sectors. This can be explained by the constant challenges in system interconnectivity and an environment of continual changes in legislation (Croll & Croll, 2006).

A hospital is an environment in which sensitive information is the base of clinical decisions, so there is the need for a correct balance between the usability of information technologies and the security of the information (Kurtz, 2003). Hospital Information Systems (HIS) need to tackle security concerns regarding confidentiality (e.g. access control, and secure communications), integrity (e.g. data consistency, error correction, redundancy, and accidental or malicious alterations) and availability (e.g. continuous access to information by authorised users).

Confidentiality, which involves access control and secure communications, has been defined as ensuring that information is accessible only to those authorised to have access (ISO, 2000).

Access control relates specifically to confidentiality, and is a step performed after the identification and authentication of users is finished. Its purpose is to guard access to the patient records in the Information Systems (IS). Access control should start with a clear and succinct definition of an access policy (Blobel, 2000). This may seem easy to achieve, but usually does not exist, either because it can be very complex or simply because no one thought it was necessary to articulate it. In the healthcare environment, processes and people acting upon them may change very often and are, therefore, difficult to track. The primary cause of security breaches is insiders and the consequences in a healthcare environment can be more damaging than in any other organisation. Security should enable and not intrude in the daily workflow; otherwise people will try to bypass it just to do their work more easily. So, it is very important to assess and understand the reality of a working environment in a hospital.

Of the few published studies on the specific issue of password management and security in healthcare systems, a previous survey (Stanton & Stam, 2005) showed that end users do not comply with the regular security procedures that are necessary to keep their user accounts' information safe. This behaviour is closely related to the organization goals, so end users from organizations whose missions depend mainly upon security, behave better in performing security procedures. Nevertheless, training, awareness and knowledge of monitoring can also help in improving users' behaviour. Unfortunately, the downside of this is the fact that end users need to remember their chosen or assigned passwords so they tend to write them somewhere in order not to forget them. Furthermore, all the awareness and training of end users seems to be of little effect when it comes to password sharing behaviours.

This chapter addresses the topic of password sharing as follows. The Background section introduces some concepts related to Electronic Medical Record security. Password Sharing section confronts and analyses case study results of what happens in practice in terms of sharing passwords. It then compares this to what the healthcare professionals say happens and what their opinions and views on these issues are. The next section (Discussion and Recommendations) discusses the results in more detail and presents some recommendations for possible solutions to the problem of password sharing, in terms of both

technological and social and cultural changes. The chapter ends with the conclusions of this research.

BACKGROUND

Information Security

Information security is usually defined by three main characteristics: *confidentiality* as the prevention of unauthorized disclosure of information; *integrity* as the prevention of unauthorized modification of information; and *availability* as the prevention of unauthorized withholding of information or resources (Gollman, 1999; Harris, 2003). In specific environments, like healthcare, some authors and even standards like the ISO 27000 family, highlight other security properties, like Authenticity (the clear identification of the author of a piece of information), but these can usually be considered as variants of the three main properties (e.g. authenticity can be considered to be part of integrity (Pfleeger & Pfleeger, 2007). Another important variant is the difference between privacy and confidentiality. Privacy relates to the right an individual to protect his or her private information from unwarranted disclosure, whilst confidentiality relates to the provision of mechanisms to protect information from unauthorized access (Gollman, 1999).

The complexity of information security systems make it very difficult to build a fully secure system (Schneier, 2004). This complexity is related to 3 contributing factors: the technology itself and the risks inherent in using it; the difficulty of classifying information in terms of both organization and users' security requirements; and facilitating the ease of understanding and use of the information technology by humans. The end users of the system are usually not technological experts and this is one of the most problematic factor to consider (Schneier, 2004) when it comes to access control. These contributing factors coupled with the fact that attackers are always finding new ways to exploit potential vulnerabilities in existing technology make it very difficult to build secure information systems. To make matters worse, potential solutions often have conflicting aims, for example: assuring the privacy of information, whilst needing to be able to access it for audit or law enforcement purposes; making it easy for an authorised user to gain access to information but complex for an unauthorised one.

Electronic Medical Record - EMR

A patient record is a set of documents containing clinical and administrative information regarding one particular patient. It supports communication and decision making in daily practice, and is used by different users for different purposes (Wyatt, 1994). It exists to memorise and communicate the data existing on a particular individual, in order to help deliver care to him or her. Records are not only an information resource but also a communication mechanism which enables communication between health professionals and between the past and the present (Dick & Steen, 1997) (Nygran, Wyatt & Wright, 1998). Patient records, the patient and published best practice are the three sources needed for the practice of evidence-based medicine (Wyatt & Wright, 1998). They are used for immediate clinical decisions (either by the author, or by others), future clinical decisions, quality improvement, education, clinical research, management and reimbursement, and to act as evidence in a court case (Wyatt, 2005). Many different names are given when patient records are computerised. Some of the acronyms found in the literature are confusing and others are redundant. Terms like Computerised Patient Record (CPR), Computerised Medical Record (CMR), Patient Health Record (PHR), Electronic Medical Record (EMR) and Electronic Patient Record (EPR) have been used in the past. Electronic Health Record (EHR) has turned out to be the most generic term, although each one of the others represents a different concept in the current

understanding of EHR (Waegemann, 2002). This chapter uses the term Electronic Medical Record (EMR), which means an organised collection of all medical records about an individual patient stored in the various computer systems and databases of all the providers who have provided health care to that patient within their organisation.

For decades, medical records' technology was remarkably stagnant. Occasional breakthroughs consisted of new systems of colour-coded chart tags and rolling lateral file cabinets (Bodenheimer & Grumbach, 2003). In 1997 it was stated that after 30 years of work and millions of dollars in research and implementation of computer systems in healthcare in the USA, patient records were still predominantly paper records (Dick &Steen, 1997). Between 1991 and 1998 the European Union provided 47 Million Euros of direct funding support to research projects on EMRs whose budgets totalled 76 Million Euros (Iakovidis, 1998). As a result of some of these efforts, EMRs were implemented in the healthcare institutions of each country, although at very different speeds. During the 80s and the 90s the free market in provision gave rise to a considerable fragmentation (Beolchi, 2002).

Generically the main requirements an electronic medical record must fulfil are:

- be fast enough to give instantaneous replies;
- have a simple interface, which is easy to use;
- be trustworthy regarding the information it delivers;
- be versatile to adapt itself to user requirements;
- be extensible to include new features as they arise.

Problems of EMR Confidentiality and Healthcare Professionals

The introduction of EMR systems within healthcare organizations has the main goal of integrating heterogeneous patient information that is usually scattered over different locations (Waegemann, 2003; Cruz-Correia 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 (MRI, 2005). This and the distributed nature of the information stress the need for information security requirements to be taken seriously (Bakker, 2004).

One obstacle mentioned by healthcare professionals for the use and integration of EMR within healthcare is the lack of controls to assure patient privacy (Knitz, 2005). As stated earlier, in order to protect a patient's privacy it is essential to at least provide for information confidentiality. Healthcare professionals report that using EMR has problems in terms of security due to its ease of distribution and wider online access (Miller, Hillman & Given, 2004). If they do not comprehend the technology or how the system can or cannot protect patient information it will be more difficult for them to agree on using it, or to help improve its flaws and integrate it efficiently within their daily work.

On the other hand, healthcare professionals normally bypass system controls in order to hasten and make the completion of their tasks easier (Lehoux, 2006) (Adams & Sasse, 1999). When they do this, they do not realize that they could be doing more harm than good. Sharing passwords is similar to sharing identities, to masquerading as another identity and performing tasks as another person. So anyone that is using another person's password will be associated to that identity. When something wrong happens, when for example someone inserted the wrong information about a patient's medication and the patient gets worse, who is the responsible party? If multiple human users are using the same user account, then the audit trail is unable to determine precisely which human user did what to which information and when. It thus becomes impossible to find the source of any security breach. However, the account holder – the person to whom the username and password was

originally issued – will be held responsible if he/she was supposed to be the sole user of the account and password sharing is officially forbidden by the organization. In this case this user is officially the only person using that username/password combination. Users typically will not want to be held responsible for unauthorized actions that they have not undertaken, and once this is made known to them, they will be unlikely to want to share their account passwords again.

Users usually have no problem in understanding that certain computer accounts should only be accessed by themselves and that their usernames and passwords should not be divulged to anyone else. If you ask users if they would be willing to give their bank debit or credit card and PIN number to someone else, they would invariably say "certainly not". Thus they have no problem in understanding that some accounts should be for their sole use only.

Password sharing may happen if there is the assumption that only registered healthcare professionals are using the system. But are they the only users? How can the systems' administrators check if there are no intruders in the system if everyone uses the same identity? The current user may be someone from outside that is trying to do harm. The intruder may only access confidential information but could, even worse, change and/or delete it. Sharing passwords distributes them and makes it easier for them to be discovered by outsiders or by insiders that are not authorized to access the EMR. It is therefore not only bad practise but also potentially dangerous practise.

Password sharing in healthcare needs a proper study and improvements in password usage must be properly adapted to the human users of EMR as well as to the technical functionalities of the EMR itself. The next section presents two studies that help to understand what really happens in practice regarding sharing passwords and reveals what healthcare professionals' feel about it.

PASSWORD SHARING

This section presents a review of published studies about password sharing from the healthcare practice and from healthcare professionals' perspectives. It also includes results from an analysis of user access logs of a real EMR system as well as from studies that explored the users' perceptions and opinions in relation to password sharing.

Literature Review

A literature review was performed according to the following steps:

1. Build search queries to select published articles of the subject in study (see Table 1).
2. Filter the published papers based on their titles and abstracts.
3. Select related papers and papers that are referenced by the ones selected in B.
4. Get the full papers.
5. Read and summarize the full papers.

A large number of papers regarding password sharing and password authentication problems were found in the initial search (see Table 1). From this list of papers there was a further selection in order to choose the papers relating to healthcare practice as well as papers regarding healthcare professionals' perspectives and views on these topics.

For the healthcare practice theme, from the 183 papers obtained from the search, after performing steps A to E, only 10 papers were selected for review, from which 9 full papers were obtained. From these 9 papers, 5 papers were found from the initial search queries while 4 papers were found as references in step C. 5 of the 9 papers were directly related to the healthcare domain while 4 were from different domains.

For the healthcare professionals' perspectives in relation to password sharing, 10 papers were selected for review. 9 papers were directly

Table 1. Database search query results

Database	Query	No of articles
PUBMED		
	password sharing	5
	authentication password	8
	password problems	15
SCOPUS		
	"sharing password"	6
	"password authentication" problems	67
IEEE Xplorer		
	sharing password	8
	password problems	2
ISI		
	"password sharing"	7
	"authentication password"	9
ACM portal		
	"password sharing"	17
	"authentication password" problems	39
	Total	**183**

selected from the search queries while 1 was selected from referenced articles (step C). Only 8 full papers were obtained, read and summarized. From these 8 papers, only 7 papers were included in this review (one of the papers related to the professionals practice and not to their views and perspectives on the subject) - 3 papers related to the healthcare domain while the other 4 were related to other domains.

In Table 2 and Table 3: * refers to papers not from the healthcare domain; $^{+}$ refers to papers obtained not directly from the search query.

What Happens in Practice

Results from the literature review, regarding password sharing in healthcare practice, showed that for most healthcare information systems, passwords are the first line of defence in keeping patient and administrative records private and secure. However, this defence is only as strong as the passwords employees choose to use. In more detail, the published articles focused mainly on three themes that are discussed below: password sharing, constraints of the healthcare domain and attitudes of healthcare professionals.

Password Sharing

A U.S. survey of non-malicious, low technical knowledge behaviour related to password creation and sharing showed that password "hygiene" (i.e. the good practices to use passwords) was generally poor but varied substantially across different organization types (e.g., military organizations versus telecommunications companies) (Stanton & Stam, 2005). The set of studied items included three items pertaining to password management behaviour (e.g., frequency of changing the password), three items pertaining to password sharing behaviour (e.g., sharing with others in the work group) and three items pertaining to organizational support of security-related behaviour (e.g. "My company/ org. provides training programs to help employees improve their awareness"). Their results showed that improvements in basic hygiene behaviours (e.g., frequent changes to one's password) are associated with training, awareness, knowledge of monitoring, and rewards; on the other hand, researchers did not find improvement in relation to password sharing behaviours.

Current systems for banking authentication require that customers do not reveal their access codes, even to their family members. A study of banking and security in Australia showed that the practice of sharing passwords does not conform to this requirement (Singh et al, 2007). For married and de facto couples, password sharing is seen as a practical way of managing money and a demonstration of trust. Sharing Personal Identification Numbers (PINs) is a common practice among remote indigenous communities in Australia. In areas with poor banking access, this is the only way to access cash. People with certain disabilities have to share passwords with carers, and PIN numbers with retail clerks.

Table 2. Summary of objectives and methods from the reviewed papers

Paper	Objective	Methods & participants	Year
A	Find a better solution for user authentication besides passwords	Survey	2003
B	Collect problems from users and staff	Online tracking system - 278	2007
C	Investigate the use of the digital pen (DP) system to collect data in a clinical trial.	Qualitative (semi-structured interviews; focus group) Quantitative (questionnaire) - 134	2008
D*	Assess how people deal with money and banking in the context of their relationships	Qualitative (open-ended interviews and focus groups) – 108	2007
E*	Family Accounts - a new user account model for shared home computers	Group interview; system use; questionnaires – 38	2008
F*	Assess students' best practices on password security	Survey	2008
G*+	Assess user behaviours and perceptions relating to password systems	Web based questionnaire – 139	1999

Table 3. Summary of the problems and solutions and/or recommendations relating to passwords

Paper	Problems	Possible solutions and/or recommendations
A	The need to remember multiple passwords	Single sign on with biometrics
B	4% (11 reports) were password problems (forget password or application not available on all computers)	Improve future implementations based on paper obtained results
C	Most of the technical problems of the system occurred during setup-password access	Improve future systems based on paper obtained results
D*	Sharing of passwords	Design security systems for banking based on observed social and cultural practices of password and pin sharing
E*	• A family who used password-protected profiles mentioned that everyone except the mother had forgotten their passwords, so they relied on her to remain logged in. • Only one study participant claimed to never use someone else's profile, while seven of nineteen (37%) claimed to use someone else's profile at least weekly. • A majority of the participants in the multiple profiles group mentioned that they use other family members' profiles for quick tasks due to convenience, if the computer is already logged in.	This user account model is the most appropriate model for using shared computers
F*	Passwords have many problems	Practices and attitudes should be improved; develop a web application to help students gaining experience with passwords
G*+	4 major factors influence effective password use: multiple passwords; password content; perceived compatibility with work practices; users' perceptions of organizational security and information sensitivity	• Designers of security mechanisms are the key to successful security systems; • Unless security departments understand how the mechanisms they design are used in practice, there will remain the danger that mechanisms that look secure on paper will fail in practice

Constraints of the Healthcare Domain

The access to patient data is not as simple as it may appear at first glance. The processes of healthcare delivery are very dynamic, and so some authors claim that the problem of access control with access control mechanisms (ACM) is too rigid to represent the staff's role and affiliate/membership in the complex real world. Consequently, it

may have been natural for a hospital to prioritize resolving that problem.

To Hirose (Hirose, 1998), this problem is caused by the security system representing neither the patient-doctor relation nor the clinical situation at the points of care. He suggested that one possible solution to this problem is to implement an access control method based on the "relation and situation" model on a multi-axial ACM. In his words, "our method holds user declaration of relation/situation as the access reason, then allows flexible data access as needed at the point-of-care. As the result, EMR system records (who, when, where, why, whose, what, and how) on each access, and has the ability of accurately audit without any maintenance cost" (Hirose & Sasaki, 2001).

This interesting solution includes a health professional / patient relation and situation model that includes the following possible classifications:

- in charge of pre-examination
- in charge
- as a member of the treating team
- on behalf of (when the staff in charge is off duty)
- on night coverage
- as a request for consultation
- in an ambulance
- in an emergency
- as an auditor

Also it includes time classifications:

- constant (e.g. main doctor or treating team staff)
- periodical (e.g. anaesthetist or ICU staff)
- intermittent (e.g. some kinds of therapeutic support)
- unsettled (ex. consultation)

Attitudes of Healthcare Professionals

In a 2006 paper, Cazier et al. presented the results of a study of actual healthcare workers' password practices (Lazier & Medlin, 2006). They have examined the passwords created by 90 employees of a healthcare agency through an empirical analysis of the passwords, the factors of length and strength. The results of this study show that a very small percentage of employees are using most of the best practices as recommended by governmental, educational and private organizations. Most users (64%) did not use both upper and lowercase passwords. The vast majority (78%) of those who do use upper and lowercase passwords, do so only in logical places, such as in capitalizing a name.

In addition to using a mix of upper- and lowercase letters, most experts recommend having a combination of letters and numbers. In this case, less than a fourth (24%) used both letters and numbers. Of those who used letters and numbers, the vast majority (82%) only used numbers at either the beginning or end of the word. Also, the great majority of the employees, 59%, appear to be using common words that can be found in any English language dictionary, thus making them very susceptible to dictionary attacks or password guessing. Of even greater concern, 43% of all passwords appear to be the name of a person. Another common threat is having the user name the same (4.4%) or similar (11%) to the password.

The authors concluded by stating that most employees in this healthcare agency were not very security savvy when they created their passwords. Also it appears that they do not completely understand the ramifications of a password breach (like possible access to patients' accounts by a hacker) and how their choice of a weak password could affect the security of their agency's system.

A Case Study

Methods

Three different Information Systems implemented in hospitals were used in this study: (1) a Virtual Patient Record (VPR), (2) an Obstetrics and Gynaecology Departmental Patient Record (ObsGyn.

care), and (3) a Hospital Information System (HIS). The first two information systems are being used in a Central Hospital with more than 1300 beds, whilst the third one is running in a smaller regional hospital with about 300 beds.

The accesses and actions taken place in each of these systems are logged in databases. The collected log data of the three information systems referred to sessions from October 2004 until December 2007. The suspicious behaviour that was searched for was users working for more than 24 hours (in some cases doctors work for 24 hours consecutively). All user sessions that started less than 10 hours from the end of the last session were considered to be referring to the same working day.

Results

The number of suspicious cases found in VPR was 508; the calculated working days ranged from 24 to 63 hours (average = 29 hours). These working days referred to 139 of 1434 logins (r_{VPR}=9.7%). In 72 logins (r_{VPR}^{1}=5.0%) the suspicious behaviour only occurred once; in 57 logins (r_{VPR}^{2}=4.0%) occurred 2 to 9 times; and in 10 logins (r_{VPR}^{10}=0.7%) occurred 10 to 56 times. The 10 logins that more frequently have suspicious behaviour referred to the following medical specialties: Anaesthesiology (4 logins), Emergency (2 logins), Infectious Diseases (2 login), Cardiothoracic Surgery (1 login), Gastroenterology (1 login).

Regarding ObsGyn.care, the number of suspicious cases found was 58; the calculated working days ranged from 24 to 48 hours (average = 27.5 hours). These working days referred to 28 of 266 logins ($r_{O\&G}$=10.5%). In 16 logins ($r_{O\&G}^{1}$=6.0%) the suspicious behaviour only occurred once; in 12 logins ($r_{O\&G}^{2}$=4.5%) occurred 2 to 9 times; and never ($r_{O\&G}^{10}$=0%) occurred more than 10 times.

Regarding HIS, the number of suspicious cases found was 315; the calculated working days ranged from 24 to 91 hours (average = 34.5 hours). The working days referred to 77 of 346 logins (r_{HIS}=22.3%). In 26 logins (r_{HIS}^{1}=7.5%) the suspicious behaviour only occurred once; in 43 logins (r_{HIS}^{2}=12.4%) occurred from 2 to 9 times; and in 8 logins (r_{HIS}^{10}=2.3%) occurred from 10 to 22 times.

The rate of suspicious cases is very similar in the VPR and Obs.care (r_{VPR}=9.7%; $r_{O\&G}$=10.5%), and is double in the HIS case (r_{HIS}=22.3%). However, in the VPR there were more recurring cases than in the Obs.care IS (r_{VPR}^{10}=0.7%; $r_{O\&G}^{10}$=0%), see Table 4.

Discussion

Although technical solutions exist to provide secure access control, they demand a clear definition of permissions for each group of actors. Healthcare organisations must comply with current legislation, ethical rules and internal processes, which are very difficult to objectively define as access control rules. The number of shared passwords found may probably just represent the tip of the iceberg. However, it is sufficient to generate apprehension.

Table 4. Comparison of password sharing among three Information Systems; number and ratio per month of cases of suspected working days (SWD); number and percentage of suspected logins, and percentages grouped the frequency of SWDs

Information System	SWD		Suspicious Logins N (%)			
	N	Per month	Total	*Once*	*Until 10 times*	*10 or more*
VPR	508	14	139 (9.7)	*72 (5.0)*	*57 (4.0)*	*10 (0.7)*
ObsGyn.care	58	2	28 (11)	*16 (6.0)*	*12 (4.5)*	*0 (0.0)*
HIS	315	105	77 (22)	*26 (7.5)*	*43 (12)*	*8 (2.3)*

The analyses of these results made the developer team of HIS change some features of the system, namely the creation of a timeout function so that the interface logs out automatically after a specific idle time. This way the interface locks out and makes the next user insert his/her credentials again. The plan is to make a new analysis of the HIS system in the future, in order to evaluate the impact of the timeout function on login and password sharing.

Healthcare Professionals' Perspectives

Results from the literature review, regarding healthcare professionals' perspectives about password sharing, showed that in both healthcare and other domains, problems with password usage are very similar (Table 3 and Table 4). These include password sharing on a regular basis as well as password forgetting. Although most studies conclude that the obtained results will help to improve the design and definition of password authentication mechanisms, this can only be achieved if the development phases focus on end users' needs and workflows. In order to further explore health care professionals' perspectives a study was carried on. It included a qualitative method (focus groups) to gain lot of information regarding this issue, followed by a quantitative method (a structured questionnaire) to further explore specific issues that came up during the focus groups' discussions.

Focus-Groups

The main objective of focus groups (FG) is to gather opinions and experiences related to specific topics. This is obtained through sampling groups (comprising 6 to 8 people) of the required population, who meet to discuss a set of topics amongst themselves. The discussion can last on average from one to one and a half hours, and is guided by a skilled moderator who records the discussions. The data is first transcribed and then analysed in a qualitative manner.

Methods

Population

The selection of participants was made from postgraduate students at the Faculty of Medicine of the University of Porto. Students were chosen from the following Masters Courses: Medical Informatics and Evidence and Decision in Healthcare; and from the Doctoral Programs in Clinical Studies and Healthcare Services Research. Both healthcare professionals (HCPs) and informatics' professionals are enrolled on the Masters Courses, but only HCPs were selected and put into groups according to their professional backgrounds (i.e. segmentation). One of these groups however had HCPs with mixed backgrounds. The doctoral program only enrols medical doctors and so these comprised one of the groups. The reason for grouping participants according to professional backgrounds facilitates discussions because all the participants in a group have similar experiences and backgrounds, usually at the same level (Morgan, 1996).

The HCP were contacted and selected at the beginning of their courses (during their first lectures). They were gathered in a room without knowing that they were going to participate in a focus group or what the topic of discussion was going to be.

Line of Discussion

The list below presents the line of discussion that was followed by the moderator:

1. The participants were given the main theme to discuss and other information regarding the process that would be followed during the course of the focus group. Each participant was asked to give their consent to participating.

2. Each participant was initially asked to give details about their profession and work location, as well as the use of EMR within their practice.
3. After that they were all asked to discuss amongst themselves:
    a. The use of paper records or EMR, what are the advantages or disadvantages of each
    b. access control issues in general
    c. access control mechanisms they use on a daily basis when accessing any system
    d. the problems and benefits of giving different access levels to different groups of users
    e. access control policies to EMR: who defines them, what should be improved

At the end they were asked to give their opinions about the best access control solutions they think should be used to control the access to EMR.

Data Collection and Analysis

Data was collected by audio recording the whole conversation while the conversations of the third and fourth group were also recorded with a video camera (see Table 5).

Regarding the analysis, only one person was involved during the whole process. The discussions from each focus group were transcribed into 4 separate word documents. Each document was then divided into smaller ones, containing only the dialogues belonging to each one of the participants, so that the data could be more easily related to a specific participant.

All documents were inserted into the qualitative analysis software, QSR NVivo 7 (NVivo, 2009), and the coding was done using this tool to register and structure data in a more automatic way. The coding started after each focus group documents were generated and was done separately for each focus group.

The data analysis was performed in phases. In the first phase, codes were generated from the data itself (in vivo coding), using a line-by-line coding strategy. These codes comprise the core ideas that were found within the text. Line-by-line coding helps to identify gaps, define actions and explicate both actions and meanings and leads to developing theoretical categories. On a second phase, a more focused and structured coding was done and codes started to fit and be grouped into categories. The third phase was based on axial coding where relations between categories and sub-categories became more visible and so they were organized as such.

Results

Four groups were arranged with a total of 26 participants: one group with 4 nurses (FG1), one group with 5 health technicians (FG2) (3 radiologists, 1 pharmacist and 1 neurophysiologist), another group with 7 people from mixed backgrounds

Table 5. Description of each focus group data collection

FG	Segmentation	Date & Time	Recording	Audio	Video	Moderators
FG1	Yes	11/01/2008 18h:20m	44m:28s	Y	N	2
FG2	Yes	11/01/2008 19h:20m	37m:22s	Y	N	2
FG3	No	21/02/2008 19h:00m	54m:44s	Y	Y	1
FG4	Yes	26/06/2008 19h:00m	40m:16s	Y	Y	1

Table 6.Healthcare institutions for the FG participants

FG	University hospital	Health centre	Hospital	Hospital centre (2 or more hospitals)	Private clinic
FG1	1	1	2		
FG2	2		2	1	
FG3	1	1	3	1	1
FG4	4	1	1	4	
TOTAL	**8**	**3**	**8**	**6**	**1**

(FG3) (1 doctor, 3 nurses and 3 health technicians) and the last group with 10 medical doctors (FG4). Table 6 shows the participants' affiliations.

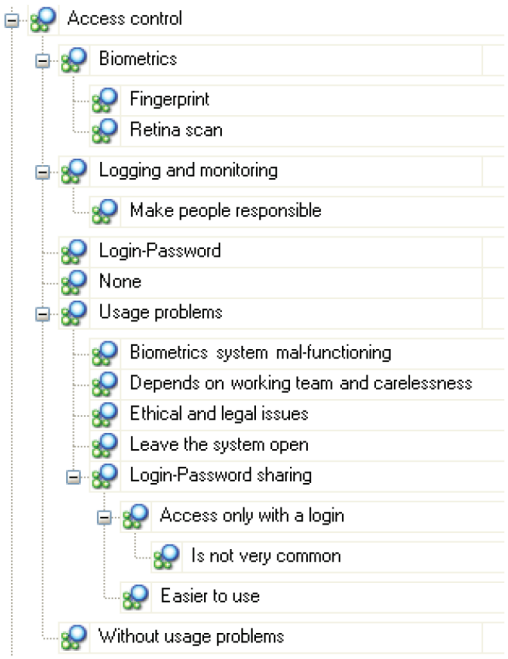
Figure 1 shows one of the main categories (access control) and sub-categories related to the topic of shared logins and passwords that came up during the focus group discussions.

From all the focus group discussions 16 different people (6 nurses, 3 health technicians and 7 doctors) talked about shared logins and passwords. 14 state that passwords are shared on a regular basis while 2 state that each professional has his own password and to use others they need to know them and it is their responsibility.

From the 14 that stated that passwords are shared on a regular basis: 3 people said that the professionals usually left the applications open and so others could still access and use the application with another person's login and password; 3 people said they needed to use a colleague's password because the system had some problems or theirs was not available at the moment; 2 people said that as they work in a team of two, they both used each other's passwords at some point; 2 people said that there was an habit of password sharing within the clinical environment; 2 people said that it was common to enter several computers at the same time with the same password; 1 person said that some applications only needed a login to access while another said that there were usually generic passwords within the applications.

Some quotes from the focus groups discussions relating to password sharing:

Figure 1. Main category and sub-categories related to the topic of shared logins and passwords, generated from the focus groups discussions



"In the beginning I didn't have a login, I had a colleague beside me and I never used his credentials without him being around…" (nurse)

"…something that happened to me was that because the IT service was not available and did not give me a login and password, my superiors told me to use another person's login and password… this is not right is it? Because I'm recording

something I did in someone else's name… it is ethically incorrect…" (nurse)

"…there is not much security at a clinical level… there is the habit of using each others' logins…" (technician)

"…It depends on the working team…where I work (health centre or hospital) no one is careful to keep their passwords secret…" (nurse)

"…people leave the applications open all the time…" (technician)

"…well, actually in my case, we usually work in pairs so the doctor with another team member… so with my password or hers..it's easier to medicate the patient, to visit the patient…is easier…"(*doctor*)-- *"In my Unit is similar…" (nurse)*

"…sometimes…to access the system we just need to provide the login…and it is possible, without a password..and is easy because the login everybody knows…it's the ID number of the professional…" (nurse).

Discussion

Although healthcare professionals are bound to preserve patients' confidentiality and deal with very sensitive information on a daily basis they refer that passwords are shared on a regularly so that they can perform their job more easily, or because they neglect the closing of the application they are using, or even because the system was unavailable and professionals needed to access it using other people's credentials.

These results show not only problems related with the technology and system efficiency and performance, but also with human processes and workflows. These problems need to be addressed both in terms of making sure system availability is guaranteed for a 24/7 period as well as changing cultural and social interactions to guarantee that healthcare professionals have more difficulty in sharing their identity. This can be done by allowing them an easier and regular access to the systems, without hindering those from achieving their main goals (i.e. to treat patients with the best resources possible available) and making them bypass the security controls.

Structured Questionnaires

These are questionnaires containing different sets of questions, organized in a specific order. A sample of the population is selected and the questions are applied either face to face or people are left to complete them in their own time. The questionnaires can be oriented to focus on specific information. They can, for instance, be based on previously obtained information such as from focus group discussions, as they were in this specific study. The data is analysed quantitatively.

Methods

Construction of the Questionnaire

Questions were constructed based directly on the categories resulting from the focus groups, with the exception of Section 3 where the topics were related to legislation and patient rights to access their medical record. Section 3 also contained questions about a hypothetical scenario.

Population

Questionnaires were tested and corrected with 5 different people from different backgrounds before they were applied to the population in the study.

Healthcare professionals from different healthcare institutions and backgrounds were approached in a random fashion at their working place during working hours. They were asked to answer the questionnaire and they could either refuse to do it, do it immediately or do it later in their own time.

Data Collection and Analysis

Data was collected from the respondents, who were completely unaided in this. The data was subsequently analysed and summarized by the SPSS statistical program.

Results

27 valid questionnaires were received and analyzed. Questionnaires were received from 12 medical doctors, 6 nurses and 9 healthcare professionals. 16 participants were female while 11 were male. 14 participants worked in a hospital, 5 in a health centre, 1 in a laboratory, 2 in an academic institution, 1 in a public healthcare institution and 4 in a private healthcare institution. In terms of academic education, 23 respondents had a BSc and 4 had an MSc. Also, 16 had some informatics' proficiency, 7 had had some informatics' education and 3 had had none (1 respondent did not answer this question).

The questionnaire was divided into four sections and was based on the categories generated from the focus groups' discussions. The questionnaire was designed to further explore some the issues that are more relevant to this study. Section 1 contained 9 generic questions regarding EMR; Section 2 had 11 questions regarding access control to EMR; Section 3 had 4 questions about a fictitious scenario of patients using an Automatic Teller Machine to access their medical records; and Section 4 had 7 demographic questions.

The answers obtained from Section 1 of the questionnaire showed that 21 HCP had used EMR during the course of their work whilst 6 respondents never had and 17 HCP used the EMR daily or almost every day whilst 3 used EMR between 1 and 3 times per week. The responses from the second set of questions focused on those 21 respondents that have used EMR during the course of their work. 19 respondents said they logged in to the EMR with a password, 4 of them used passwords together with biometrics, 1 respondent used biometrics alone and 1 did not use any kind of mechanism.

Table 7 summarises the responses from the most common issues when users authenticate to the EMR with username and password. 15 said this mechanism was easy to use, 4 said they usually share their usernames and passwords, 3 continually forget their passwords and 2 had no opinion on the subject.

Discussion

Although many references were made during the focus groups' discussions in relation to sharing passwords as a common practice amongst the healthcare professionals, only 4 people from the 21 that use EMR for their work agreed that they share passwords. This can mean that when people are asked about the fact itself they may not want to refer it as something they do but when discussing it on an informal way amongst other professionals, this is regularly mentioned, even if in the third person as "something that happens regularly".

Again, healthcare processes and workflows need to be analysed in depth so this issue can be tackled and corrected according to user needs and goals when using the systems.

DISCUSSION AND RECOMMENDATIONS

Interpretation of the Studies

The studies showed that healthcare professionals are aware of what happens in practice and that sharing passwords is a common behaviour. Although

Table 7. Issues regarding the use of login and password as authentication mechanisms

Issues of login-password	No of respondents
Accesses easily	15
Shares passwords	4
Forgets many times	3
No opinion	2

some see it as a wrong behaviour others feel that it can be a useful strategy to fasten and facilitate the team work. The use of passwords as an authentication mechanism is very easy to implement and use but may not be the most efficient mechanism to protect information. It is also very difficult to control, in practice, who shares passwords with whom since the records can only show the identity that accessed and when. This means only an identity can be verified and not who physically accessed the system. A brief study of the access control logs can be one first step to verify if this problem may or may not exist. If the problem is suspected to exist, then other measures can be introduced according to the system's objectives and security level. These measures are further discussed in this section where some technical and well as social and cultural recommendations are presented.

How to Reduce Password Sharing

The issue of password sharing can be addressed from two different perspectives. One is the technological perspective; the other is the human perspective. Whilst different technologies can be used to help to stop the problem of password sharing, without the active involvement of the human users, many technological solutions might fail. Consequently this section will first address the human aspects of password sharing, and then it will turn to the different technologies that might be used to help to address the issue.

Social and Cultural Suggestions

It is abundantly clear that password sharing can only be reduced through the active involvement of the human users. Unless users are willing to acknowledge that password sharing is a problem that needs to be addressed, then little progress will be made in eradicating it (other than by technologically eliminating the need for passwords). EMR are a critical resource to organizations in the health sector. If these records were to become publicly available and broadcast on the Internet, or were to be tampered with by intruders without the knowledge of the health care professionals, this could have life threatening consequences to the patients. They thus need to be strongly protected.

- A critical success factor in reducing password sharing is therefore user education (Adams & Sasse, 1999). Primarily users need to be informed why password sharing is a problem. If the users do not perceive that a problem exists, then they will not be motivated to address it. The educator needs to explain to the users that computer resources and the information that is stored on them are valuable resource to the organization;
- Part of the task of user education is to instil in users the fact that this principle should apply to all the computer accounts that they possess, and not just to their bank accounts. Consequently users should not divulge to third parties their usernames and passwords of any accounts that grant access to computer systems;
- Organizations need to have detailed audit trails recording who accessed and processed which information and when. If there is a breach in the security, it is the audit trail that will inform that and lead back to the source of the breach. (For example, a doctor or a patient will not usually know if some unauthorized person read or copied the patient's medical record, but the audit trail should have a record of this. If each access is uniquely recorded in the audit trail, and each user has a unique account protected by its own username and password, then the audit trail can lead us back to the user account which was responsible for the breach in security);
- Clearly for non-sharing of passwords to be effective, organizations need to have

sensible policies for the allocation of new accounts to users, and simple procedures to follow that are not unduly onerous or deemed to be unnecessary;

- Staff should know how to apply for new accounts (so education is important) and the procedure should be fast and efficient, so as to not de-motivate staff. (Ideally this procedure will be one that is automatically carried out when a new member of staff joins the organization, and the account username and password will be issued along with keys to doors, uniforms and other equipment that is necessary for the person to perform their roles.
- The policies for new account creation should not be too restrictive or exclusive, otherwise users may be forced into sharing their passwords so that others who are refused their own accounts, can still do their jobs in the normal way);
- If the organization is licensing software or services from third parties, and pays a license fee per user account, then the organization should purchase sufficient licenses so that all users can have their own account and consequently do not need to share the same account password. (Skimping or cheating on licenses will not encourage users to not share their account passwords on other accounts which are not so restricted);
- The culture of the organization may need to be addressed. A culture that allows staff to share confidential information between them without proper authorization will have difficulty in preventing its staff from sharing their usernames and passwords;
- The organization should also have a set of sanctions that are applied to staff who break the agreed norms of information protection and handling. Staff will be knowledgeable about the policies and correct procedures to follow, and will actively follow them;
- When passwords are lost or forgotten, which invariably they will be, there needs to be a simple, quick and efficient procedure for replacing them. Some IT Help Desks find that password replacements are the single most costly procedure that is undertaken, due to the scale of the problem. The administrator should have a single command that they can issue, which will automatically generate the new password, and print it off for the staff member to take away with them. This should be a random one-time use password that requires the user to register his/her own preferred and easy to remember password after using this newly generated password to login;
- The organization needs to have a clear and easy to understand password policy that is made known to staff and that has been agreed with them. Password policies should contain rules for the length and content of passwords, and the frequency at which they should be changed. Sample password policies are available on the Internet e.g. at http://www.sans.org/resources/policies/Password_Policy.pdf and http://password-manager.hitachi-id.com/docs/password-policy-guidelines.html. But beware. Some organizations make impossible demands on their users. They require passwords to be strong, i.e. long, in a mixture of lower/upper case, numbers, letters and non-alphanumeric characters, so that they cannot be easily cracked, and they also require them to be changed frequently to give hackers less time to crack them. This combination makes it extremely difficult for users to remember what their original strong passwords are (since they cannot be dictionary words), and the frequent change of passwords means that if a user does eventually manage to memorize his password, then no sooner has he done this than the password has to be replaced

with another one. If passwords are to be very strong then they should be granted a long lifetime measured in years rather than months, since the time taken to crack them will typically be measured in millions of years;

- Users should not have to remember multiple strong passwords as this is beyond their mental capacities. (Adams & Sasse, 1999) presents the results of a survey into user's attitudes and perceptions of passwords, and reasons for why they often break the rules.

Technical Suggestions

Technology can help alleviate the problem of password sharing, by employing various techniques that either help users to stop sharing passwords, or remove the need to use passwords. In the former category we have single sign on systems and resource management mechanisms. In the latter category we have biometric authentication, and the use of various hardware devices that do not use conventional passwords for authentication.

Helping Users to not Share Passwords

There are several techniques that can be employed to discourage users from sharing their passwords:

- **Single Sign On (SSO) is one option**. With SSO, the user's username and password are used to grant the user access to all (or as many as possible) of his accounts and applications. This has a number of benefits. Firstly it makes easier for users to move between systems, services and machines because once he has logged into the first of these, he can move seamlessly between them all without needing to login again. Clearly a user is unlikely to give his SSO username and password to a colleague, if this means his colleague is simultaneously granted access to all of his accounts. Secondly the use of just one SSO password encourages the user to utilize a much stronger password comprising more characters and more entropy than in the case where the user is burdened with having to remember many different passwords for many accounts. This adds to the overall security of the system. (However, SSO also has its disadvantages. One can regard SSO as the user putting all his computer account eggs into one basket – if an attacker gains access to one account he has access to all of them. Furthermore SSO is operationally difficult to achieve since a user's employer typically will not have access to all the user's accounts and therefore is not in a position to enable SSO to all of them. SSO is also technically difficult to achieve. This is because most organizations will have a number of legacy systems and applications which will be very difficult and costly to provide with SSO functionality);
- **Ensuring each system is scalable to the number of users that are envisaged** is also an important factor in helping users to stop password sharing. If the system itself cannot support the number of current or envisaged users, then the system administrator will be forced to make multiple users share the same account and password;
- **If the amount of resources that can be consumed by a single user account is limited**, or is charged for, then **this also discourages users from sharing their account passwords**. For example, the account could have a maximum session time, or CPU usage. If a user is likely to be restricted in his future actions because of the resources consumed by one of his colleagues to whom he has shared his account password, then the user will be less likely to share his password with others in future.

Removing the Need for Passwords

Password based authentication is relatively easy for users to understand and use, and it is easy to implement. This is why password based systems are so prevalent today. However, from a security perspective, user passwords are a very poor authentication technique. This is because passwords are easy to forge using password cracker software, they are easy to share, and users are usually unaware when they are stolen. Many alternative authentication techniques exist, which rely on either the biometric characteristics of the user or the user possessing a hardware token of some sort.

- There are many different **biometric authentication techniques** in use today (Harris, 2003), which might rely on physical user characteristics, like fingerprints, voice or iris scanning, or behavioural characteristics, like keystroke dynamics, pointer dynamics or gait (Magalhães & Santos, 2008), to name a few. Despite the characteristic being used, they all share the following properties: universality (everyone should possess the characteristic; uniquely (no users share the same biometric characteristic); continuity (the characteristic should remain unchanged); and must be measurable in computer terms (Jain & Ross, 2006). Observing these properties the biometric technique should be able to differentiate between one user and another.
- Various different types of **hardware device** can be used for user authentication. These rely on a secret computation being performed in the hardware, and the answer is provided as the user's authentication token to the system being accessed. The answer can be a onetime password or a digital signature. If the hardware device is something the user permanently needs to have in his possession, such as a mobile phone or identity card, then using this as the authentication hardware device makes it much less likely the user will share it. To stop hardware devices from being stolen and used by the thief they are usually protected with a PIN. The user has to enter the PIN into the device before it will reveal the secret to him. Entering the wrong PIN a small number of times will usually lock the device from further use. This is to protect it from being used by a thief who would otherwise try every PIN combination until he found the correct one.

CONCLUSION

This chapter presents a number of cases and experiences relating with password sharing in healthcare. The idea was to give an overview of what happens in practice and what may be able to be improved regarding this important issue. Further, the authors wanted to provide a set of suggestions to aid organizations in their quest to reduce the frequency of password sharing that is either surreptitiously or knowingly carried out by their employees. Whilst technical solutions can be employed, the most cost effective solutions are usually not technical but rather are social and cultural. The most important factor is user education. Users are typically intelligent rational human beings, and when something is properly and effectively communicated to them, such as the negative aspects of password sharing, they are usually willing to comply with the request to cease such activity.

REFERENCES

Adams, A., & Sasse, M. A. (1999). Users are not the enemy. *Communications of the ACM*, *42*(12), 40–46. doi:10.1145/322796.322806

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. *International Journal of Medical Informatics*, *73*(3), 267–270. doi:10.1016/j.ijmedinf.2003.11.008

Beolchi, L. (2002). *Telemedicine Glossary* (4th ed.). Belgium: European Commission.

Blobel, B. (2000). Authorisation and access control for electronic health record systems. *International Journal of Medical Informatics*, *73*(3), 251–257. doi:10.1016/j.ijmedinf.2003.11.018

Bodenheimer, T., & Grumbach, K. (2003). A Spark to Revitalize Primary Care? *JAMA: the Journal of the American Medical Association*, *290*, 259–264. doi:10.1001/jama.290.2.259

Cazier, J., & Medlin, B. (2006). How secure is your information system? An investigation into actual healthcare worker password practices. *Perspectives in Health Information Management*, *3*(8).

Croll, P., & Croll, J. (2006). Investigating risk exposure in e-health systems. *International Journal of Medical Informatics*, *76*(5-6), 460–465. doi:10.1016/j.ijmedinf.2006.09.013

Cruz-Correia, R., Vieira-Marques, P., Costa, P., Ferreira, A., Oliveira-Palhares, E., Araújo, F. (2005). Integration of Hospital data using Agent Technologies – a case study. *AICommunications special issue of ECAI, 18(3)*, 191-200.

Dick, R., & Steen, E. (1997). *The Computer-based Patient Record: An Essential Technology for HealthCare*. Washington: National Academy Press.

Gollman, D. (1999). *Computer Security* (1st ed.). New York: John Wiley & Sons.

Harris, S. (2003). *CISSP Certification All-in-One Exam Guide* (2nd ed.). New York: McGraw-Hill Osborne Media.

Hirose, Y. (1998). Access control and system audit based on patient-doctor relation and clinical situation model. *Medinfo'98, 2*, 1151-1155.

Hirose, Y., Sasaki, Y., & Kinoshita, A. (2001). Human resource assignment and role representation mechanism with the cascading staff-group authoring and relation/situation model. *Medinfo*, *10*(1), 740–744.

Iakovidis, I. (1998). From electronic medical record to personal health records: present situation and trends in European Union in the area of electronic healthcare records. *Medinfo*, *9*, 18–22.

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

International Organization for Standardization. International Standard ISO/IEC 17799. (2000). Information technology - Code of practice for information security management. Geneva: ISO2000.

Jain, A., & Ross, A. (2006). Biometrics: A tool for information security. *IEEE Transactions on Information Forensics and Security*, *1*(2), 125–143. doi:10.1109/TIFS.2006.873653

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

Kurtz, G. (2003). EMR confidentiality and information security. *Journal of Healthcare Information Management*, *17*(3), 41–48.

Lehoux, P. (2006). *The Problem of Health Technology: Policy Implications for Modern Health Care* (1st ed.). Routledge.

Magalhães, S., Santos, H. M. D., et al. (2008). Keystroke Dynamic and Graphical Authentication Systems. *Encyclopedia of Information Science and Technology*, Second ed. M. Khosrow-Pour. USA, Information Science Reference, 1, 2313 - 2318.

Miller, R., Hillman, J., & Given, R. (2004). Physician use of IT: results from the Deloitte Research Survey. *Journal of Healthcare Information Management*, *18*(1), 72–80.

Morgan, D. (1996). Focus Groups. *Annual Review of Sociology*, *22*, 129–152. doi:10.1146/annurev.soc.22.1.129

NVIVO 7.(2009). *QSR International*. Retrieved from: http://www.qsrinternational.com/. (13th April 2009).

Nygren, E., Wyatt, J., & Wright, P. (1998). Helping clinicians to find data and avoid delays. *Lancet*, *352*, 1462–1466. doi:10.1016/S0140-6736(97)08307-4

Pfleeger, C. P., & Pfleeger, S. L. (2007). *Security in Computing* (4th ed.). Prentice Hall.

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

Singh, S., Cabraal, A., Demosthenous, C., Astbrink, G., Furlong, M., et al. (2007). *Password sharing: implications for security design based on social practice*. In Proceedings of the SIGCHI conference on Human factors in computing systems, pp. 895-904.

Stanton, J., & Stam, K. (2005). Analysis of end user security behaviors. *Computers & Security*, *24*(2), 124–133. doi:10.1016/j.cose.2004.07.001

Waegemann, C. (2002). *Status Report 2002: Electronic Health Records*.

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

Wyatt, J. (1994). Clinical data systems, Part 1: Data and medical records. *The Lancet, 344*, 1543 7.

Wyatt, J. (2005). *Clinical data capture and presentation*. Porto: Medical Informatics Summer School.

Wyatt, J., & Wright, P. (1998). Design should help use of patients' data. *Lancet*, *352*, 1375–1378. doi:10.1016/S0140-6736(97)08306-2

ADDITIONAL READING

Brogan, M., Lin, C., Pai, R., & Kalet, I. (2007). *Implementing A Mandatory Password Change Policy at an Academic Medical Institution*. Proceedings of AMIA Symposium, 884.

Bruce, P. (2003). Rx for password headaches: biometric authentication solution lets physicians be their passwords. *Health Management Technology.* St. Vincent Hospitals and Health Care Center Inc.'s solution.

Cruz-Correia, R., Vieira-Marques, P., Ferreira, A., Almeida, F., Wyatt, J., & Costa-Pereira, A. (2007). Reviewing the integration of patient data: how systems are evolving in practice to meet patient needs. *BMC Medical Informatics and Decision Making*, *7*, 14. doi:10.1186/1472-6947-7-14

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. *Studies in Health Technology and Informatics*, *121*, 176–182.

Ferreira, A., Cruz-Correia, R., Antunes, L., & Chadwick, D. (2008). Security of Electronic Medical Records. In Lazakidou, A., & Siassiakos, K. (Eds.), *Handbook of Research on Distributed Medical Informatics and E-Health*. Medical Information Science Reference.

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?* Proceedings of the 19th IEEE Symposium on Computer-Based Medical Systems, pp. 847-851.

Ferreira, A., Cruz-Correia, R., Antunes, L., Palhares, E., Marques, P., Costa, P., & Costa-Pereira, A. (2004). *Integrity for Electronic Patient Record Reports*. Proceedings of the 17th IEEE Symposium on Computer-Based Medical Systems, 4-9.

Ferreira, A., Cruz-Correia, R., & Costa-Pereira, A. (2004). *Securing a Web-based EPR: An approach to secure a centralized EPR within a hospital*. Proceedings of the 6th International Conference on Enterprise Information Systems, 3, 54-9.

Ferreira, A., Cruz-Correia, R., & Costa-Pereira, A. (2007). *Why teach computer security to medical students?* Proceedings of the 12th MEDINFO Congress, 129, 1469-1470. Amsterdam: IOS Press

Hart, D. (2008). Attitudes and practices of students towards password security. *Journal of Computing Sciences in Colleges*, *23*(5), 169–174.

Littlejohns, P., Wyatt, J., & Garvican, L. (2003). Evaluating computerised health information systems: hard lessons still to be learnt. *BMJ (Clinical Research Ed.)*, *326*, 860–863. doi:10.1136/bmj.326.7394.860

Miller, R., & Sim, I. (2004). Physicians' use of electronic medical records: barriers and solutions. *Health Affairs*, *23*(2), 116–126. doi:10.1377/hlthaff.23.2.116

Proctor, R., Lien, M., Vu, K., Schultz, E., & Salvendy, G. (2002). Improving computer security for authentication of users: Influence of proactive password restrictions. *Behavior Research Methods, Instruments, & Computers*, *34*(2), 163–169.

KEY TERMS AND DEFINITIONS

Authentication Mechanism: A mechanism that allows the users to identify and prove who they say they are to an information system (e.g. with a login and password).

Electronic Medical Record: A set of documents within an information system, containing clinical and administrative information, regarding one particular patient in order to support the healthcare professional in his/her daily practice in treating the patient.

Information Security: Usually defined by 3 characteristics: confidentiality – prevent access from unauthorized users; integrity – prevent modification from unauthorized users; availability – provide access to authorized users whenever is needed; as well as auditing – register and control of who does what within the system; and accountability – make users responsible for what they did within the system. The last two are only possible if we can identify and trust that identities are not shared.

Login: A unique tag that identifies a user of an information system (it can be a number or a word).

Password Sharing: The act of giving the login and password to be used by another user and not keeping them private. In this way, users can act on other people's behalf.

Password: A word or string of characters that is uniquely related with a login and proves the identity of a user to the information system (this piece of information has to be kept private and proves to the system that the user identified by that login and that password is who he says he is, because this combination is unique).

Privacy: The right an individual has of keeping his/her information private. He/she controls who can access what. Confidentiality provides for privacy as it relates to the means and mechanisms put into place to guarantee that the information is kept private.

Security Breach: Security incident that violates the protection of some information. Violation may happen in terms of confidentiality (unauthorized access), integrity (unauthorized modification) and availability of information (deny of access to the information) (e.g. password sharing can constitute a breach of any of the characteristics above).