IDEA GROUP PUBLISHING

701 E. Chocolate Avenue, Suite 200, Hershey PA 17033-1240, USA
Tel: 717/533-8845; Fax 717/533-8661; URL-http://www.idea-group.com

ITP4960

Information Security in Electronic Medical Records: A Case Study with the User in Focus

Rose-Mharie Åhlfeldt
Department of Computer Science, University of Skövde, P.O. Box 408, S-541 28 Skövde, Sweden, rose-mharie.ahlfeldt@ida.his.se

Lena Ask
Department of Computer Science, University of Skövde, P.O. Box 408, S-541 28 Skövde, Sweden, lask@telia.com

ABSTRACT

Healthcare manages a large amount of information, which represented in different forms is a necessity for the healthcare work. Furthermore, security is an obvious requirement for almost everything one does in healthcare. Information are available quicker and easier by means of modern information technology (IT) but IT also entails new demands on information security awareness. It is obvious, from different sources and earlier work in this area, that user behavior is one of the most important reasons for present shortcomings in information security. This paper reports on experiences from a case study at a hospital in southwestern Sweden. The aim with the work was to determine how users, using electronic medical records (EMR), are affected by the requirements of information security, how they affect the information security, and how they obey the recommendations and common advice for processing of personal data compiled by the Swedish Data Inspection Board. The result from this work shows that users are indeed affected by, and affect the requirements of information security. This is due to, above all, insufficient knowledge about information security, but also because security policies and routines in the organization are inadequate. Consequently, users are still a critical factor when information security measures are applied in healthcare.

INTRODUCTION

Healthcare is in a state of change. Economical and demographical conditions change and new forms of healthcare and medical techniques are added. Despite this, the full utilization of IT in healthcare is still lacking. This depends on the complexity of ways of working and of organization, but also on conservatism. It is necessary to understand that in a short term, IT investments will become costly, but that in the long term, IT support is a necessity. It will generate cost savings due to more efficient work routines and information management, but most importantly, it will increase the quality of healthcare (Collste 1997).

Different threat and risk analyses have shown that deficiencies in the staff's responsibility division, organization, and knowledge, are the strongest reasons for malfunctioning IT-systems. Furthermore, analyses have also shown that own staff is the biggest risk for a conscious incorrect management of IT-systems. In addition, it is also shown that most security violations are committed by the internal personnel (Dahlin & Arnesjö 1996).

In 1998, the Swedish Data Inspection Board (DIB) published a report concerning processing of personal data in hospitals (Datainspektionen 1998). In the report they provide recommendations regarding the basic security measures for the controller of personal data in healthcare. From these recommendations and the basic functions of authentication, allocation of authority, secrecy, integrity, non-repudiation and traceability, and in order to guarantee the information security, it is important to investigate how the users follow these recommendations. In addition, various authors (Furnell et al. 1996; Lagerlund 1999) claim that users constitute the greatest risk concerning information security.

The aim of the work reported in this paper was to determine how users, using electronic medical records (EMR), are affected by the requirements of information security, how users affect the information security, and how they obey the recommendations and common advice from the DIB. The work was conducted as a field study including observations and interviews with healthcare staff at a hospital in the region “Västra Götaland” in southwestern Sweden.

The paper presents and discusses the results from this study. The outline of the paper is as follows: firstly, a brief description of information security in healthcare is given. Thereafter, the results of the study are presented and discussed. Finally, some concluding remarks and possible future research are presented.

INFORMATION SECURITY IN HEALTHCARE

Information Security in healthcare is a concept that is difficult to define even for those working with healthcare. Information in different forms is a necessity for the work, and security is an obvious requirement for almost everything one does in healthcare. Irrespectively of whether it is a computerized or a non-computerized system that is handling the information, information requirements should be the same.

To reach good information security, it is not enough with technical solutions in the system. Also, a structured way of working is required. The work must be established as a continuing process from the demands of the business to the build up and maintainenance of a conscious and adapted level of information security (Lagerlund 1999).

One secrecy problem is when a user forgets to log out from the system and the next user can use information with no allowance to access. There is a risk that employees reveal their passwords to someone who uses it for crime (Sågänger and Utbult 1998). According to Furnell et al. (2000), 26 % of the users must remember passwords and user names to five or more applications. It is a problem for the users to remember so many passwords. Consequently, the users choose simple and well-known names which are easy to remember. Dowland, et al. (1999) mentioned in their paper that 29 % of the people asked in their investigation admitted that other people know their passwords. If there are any suspicions about employees having exceeded their authority to sensitive information, it is possible to get the user name from the logging register to check if the employee have done something wrong (Sågänger and Utbult 1998).

RESULTS

This section will provide an account of the study the observations made and a summary of the conducted interviews. 30 log-on events were observed and 5 people were interviewed. A more detailed description of observations and interviews can be found in Ask (2002).

Observations

When users are going to log-on to the system, they have to use a user name and a password to access the server. Depending on which program they are going to use, they must use their user name and password once again. These passwords can be the same. The users remember their passwords and it seems that they do not need any support for the memory. Several times when the users start the computer and log-on to the system they complain that this procedure take too much time. Especially, when they are going to write just a simple note in the EMR, the log-on procedure takes the main part of the time. The users are often interrupted when they are going to write notes in the record and must leave their working place for other tasks. At such times it happens that they do not log out from the system. Hence, both unauthorized employees and outsiders can have access to patient information. This is inconsistent with recommendation and common advice from the DIB.

10 % of the log-on events, it occurred that users allowed other users to use their identity and authority. It is obvious that some users do not really understand why the log-on procedures and authority control systems exist. Furthermore, when users write notes about patients they do not use any support for the memory. As mentioned above, they are often interrupted by calls from telephone or patients who need help. Therefore, the users' ability to remember things is a challenging task when they are managing information about several patients at the same time.

Patient information was available in various places at the nurse office, and not only the computerized patient record. There are medical lists, admission notes etc. which can easily be available for unauthorized people. On the other hand, the computer screens were placed in a way such that passing-by people could not see sensitive information without entering the office. This is according to the DIB recommendations.

Facsimiles are frequently used to transfer patient information to other care units. This information is not encrypted and only in some occasions the information is unidentified. The staff makes calls to the receivers before they transfer the message and then receives an acknowledgment afterwards, telling them that the message has gone to the right person.

Interviews

There is no specific training program for information security in the organization. When users begin their employment they receive an introducing documentation from the system administrator including some security advice. Furthermore, the organization does not follow up that the advice is obeyed. The users need more continuous security information since they do not really understand their obligations concerning log-on functions etc.

Several of the interviewed persons have used someone else's identity when they make notes in the record. In various situations it has happened that they thought they had logged on to the system in a correct way, but find out when they were going to sign the record note, that this was not the case. Another example of such a situation is when users have too much work to do. The organization has no routines to check whether the users use their own user names or not. Instead, the staff is responsible for the written information in the EMR or other applications which is signed with their own identity.

In the EMR no indication is given that the user must change their password, but in the network system they must change the password every sixteenth day. The employees have various passwords to remember. The interviewed persons use 3-4 passwords and they were all, except for one user, related to relatives or similar and then combined with numbers.

Every transaction in the system is logged. The administrator has a computerized application to check the log file but there are no routines for managing the logging procedure and the log file has never been checked.

When the availability to the EMR is interrupted, it causes irritation and frustration to the staff. The interviewed nurses claimed that it will create chaos. It causes a lot of trouble since they do not have the information they need. If they get information about an interruption, they replicate all needed records and put them in a cover, and then record the new notes in the EMR afterwards. All nurses claimed that this is not a suitable way of working.

DISCUSSION

Information management should be done in a way that generates more security for the patient and such that the healthcare staff is allowed to spend more time to take care of and treat the patient, which is their primary task.

The result of the study shows that necessary actions from an information security perspective have not been taken. According to France (2001) the main part of the staff is not aware of how they are going to manage the EMR and the common information security problems when they arise. The result from this work shows the same.

The users are affected by the requirements of information security when

- *the log-on function does not work satisfactorily*, for example, the log-on routine does not fit the users' way of working, the password-exchange routine in the system is not adequate, the log on and log out routines take to much time, and it is difficult for the users to remember the passwords.
- *the users are not aware of or have not adequate knowledge about information security issues*, for example, various regulations and statutes, various functions in the systems, and risks and threats.
- *they use log-on and log out routines of the system*, in order to support traceability.
- *interruption to EMR occurs*.

Users can, as a result of ignorance concerning information security and computers, and due to the practice of sending facsimile message, be affected negatively since they do not understand that they are acting in a wrong way. They can take part in an incorrect action without knowing that the action is wrong and without understanding that they may be made responsible.

Users are not aware that IT-systems in healthcare are logged and how the organization manage and check the log. According to Engström (2002) the users have the right to training and information about routines of the organization concerning how they manage and check the log file and also what kind of data that is stored. The users are positive to have the system logged. Partly, because they want the patients' trust for the work they perform and partly, for their own safety. This implies that the users do understand reasons to log sensitive information in healthcare systems.

The result also shows that there is a problem to remember several different passwords. This implies that users use simple passwords often related to relatives' names. This is also confirmed by Furnell et al. (2000). Furthermore, the users do not have any indication from the EMR telling them that it is time to change their passwords. Consequently, users forget to do this.

When the availability of the EMR is interrupted, the users are affected negatively. Interruptions mean more work for the staff since they are forced to do redundant registrations of patient information. Still, the staff is positive to the EMR since comparing to the paper based records, the availability to patient information has been improved.

The user affects information security in EMR when

- *the log-on and log out functions do not work satisfactorily*, for example, the user leaves the computer for other tasks without logging out from the system. Also, users use other users' identities and authorities.
- *information is handled and registered in a wrong way*, for example, users forget print-outs at the printer; users do not check the receiver's authority to access information; users register information on wrong patients or send patient information by facsimiles without hiding which patient the information con cerns.
- *deficiencies in and no adequate knowledge about,* for example, application in use and why it is necessary to register information in several places in the EMR; routines for signing records and managing passwords.

The EMR's requirement on users to log on and log out with their user identity is not followed every moment. The users are not always aware of the risk when they do not log out from the system or leave their own identity to another employee. The tendency not to log out from the system because it is impractical must be changed. If not, the deficiencies will increase. Training is one way to change the bad log on routines, but the management of the organization has the responsibility to allocate time for the users and to give them information about the existing security routines. Furthermore, simple and secure log-on and log-out techniques must be purchased and implemented in the organization. The DIB (1998) pointed out in their report that the systems must not contribute to unsuitable use of authority control systems by slow and complicated log on and log out procedures.

The work also shows that an adequate and continuous training program concerning information security is needed. Security can only be received if the whole staff understands and accepts necessary security measures. Appropriate security training and attention is necessary in order to get the staff to understand the consequences their actions may have against the security (Furnell et al. 2001; Björner 2000).

The results show that users are still an important risk factor when it comes to information security since requirements for how information security is reached are not always followed by the users. The users are in need of continuous information and training about information security in order to be aware of existing risks and threats when managing sensitive information. The log on and log out functions should as far as possible support the users' way of working, instead of being a hindrance. Furthermore, users should be aware of their own responsibility when they get authority to more information than they need when treating the patient. In order to preserve and reinforce the patients' confidence, healthcare should strive for information security aware users.

CONCLUSION AND FURTHER RESEARCH

From the observation and interview results accounted for above, we conclude that users are affected by, and affect the requirements of information security. This is due to, above all, insufficient knowledge about information security, but also because security policies and routines in the organization are inadequate. Consequently, users are still a critical factor when information security measures are applied in healthcare.

The question must be asked why it is so hard to commit resources to training programs etc. for the staff. Even if various sources, both from national agencies (Datainspektionen 1998; Björner 2000) and the research community (Gratte 1996; Faulkner 2000; Furnell et al. 2001) have stated these facts for several years, this work shows that the situation is still the same. Concerning training, there are no direct gains that immediately appear in the budget. In contrast there is another set of values than the clearly economical ones that must be observed. If it is hard to reserve resources for education when there are clear economical gains, it seems to be even more so when there are no such direct gains (Åhlfeldt 2001).

From the above, it may be claimed that it is important to conduct further research on the resources needed, for the staff to be able to acquire sufficient knowledge about information security matters. Furthermore, imagine an ideal world in which these resources have been made available for staff's training, would that naturally lead to a sufficient awareness on information security or are there any other factors that also come into play?

Another possible future research issue would be to investigate how and why it is so hard to implement simple and efficient log-on and log-out functions, for example, smart cards, single sign-on techniques etc, although it clearly facilitates the daily work for the staff.

It would also be interesting to relate our results with experience from other countries in similar areas in healthcare, for example, to compare Swedish regulations to the HIPAA standards and the users' role in it.

Information security in EMR is a part of the whole information security thinking in healthcare. A satisfying security as a whole is a demand according to national regulations. To fulfill this demand, the users must be taken into account.

REFERENCES

Ask, L. 2002. "Informationssäkerhet i datorjournal – en studie med användaren i fokus", Bsc dissertation HS-IDA-EA-02-303, Institutionen för Datavetenskap, Högskolan Skövde, 2002 (in Swedish).

Björner, O. 2000. *"Tjänster för att uppnå informationssäkerhet i hälso- och sjukvården"*, Rapport nr 3 från SITHS-projektet, 1999 (in Swedish).

Collste, G. 1997. Vårdens datorisering ur etiskt perspektiv. I: Arensjö, B., Lagerstedt, M. & Nilsson, G. (Eds). *IT i vården*, Sveriges Utbildningsradio AB, chapter 4 (in Swedish).

Dahlin, B. & Arnesjö, B. 1996. Datorjournalen. In: Petersson, G. & Rydmark, M. (Eds). *Medicinsk Informatik*, Liber Utbildning AB, chapter 6 (in Swedish).

Datainspektionen, 1998. Person-regi-strering vid sjukhus, Datainspektionens rapport December 1998 (in Swedish).

Dowland, P.S., Furnell, S.M., Illingworth, H.M. & Reynolds, P.L. 1999. Computer crime and Abuse: A Survey of Public Attitudes and Awareness. *Computers and Security, 18,* pp. 715-726.

Engström, S. 2002. Arbetsmiljö. Föreläsningsanteckningar i kursen Informationssystem inom vården, Högskolan Skövde 2002-05-02 (in Swedish).

Faulkner, X. 2000. *Usability Engineering*, London: Macmillian Press Ltd.

France, R. 2001. Security Of Electronic Health Care Records: A Clinical Perspective I: The ISHTAR Consortium. *Implementing Secure Healthcare Telematics Applications in Europe* (s.23-31). Amsterdam, IOS Press, volym 66, chapter 2.

Furnell, S.M., Gaunt, P.N., Holben, R.F., Snaders, P.W., Stockel, C.T. & Warren, M.J. 1996. Assessing staff attitudes towards information security in a European healthcare establishment. *Medical informatics, 21,* pp. 105-112.

Furnell, S.M., Dowland, P.S., Illingworth, H.M. & Reynolds, P.L. 2000. Authentication and supervision: A Survey of User Attitudes. *Computer and Security, 19,* pp. 529-539.

Furnell, S.M., Warren, M.J. & Evans, M.P. 2001. The ISHTAR World Wide Web Dissemination and Advisory Service for Healthcare Information Security I: The ISHTAR Consortium. *Implementing Secure Healthcare Telematics Applications in Europe,* pp. 249-281. Amsterdam, IOS Press, volym 66, chapter 9.

Gratte, I. 1996. *Datorn i vården*. Falköping. Liber Utbildning AB (in Swedish).

Lagerlund, B. 1999. *"Informations-säker-het i vårdprocessen: Krav beskrivna i generella användningsfall utifrån vård-scenarion"*, Rapport nr 1 från SITHS-projektet, 1999 (in Swedish).

Sågänger, J. & Utbult, M. 1998. *Vårdkedjan och informationstekniken*, Teldok rapport 199 (in Swedish).

Åhlfeldt, R. 2001. Information Security in Home Healthcare – Personal Integrity and Secrecy, Msc dissertation, HS-IDA-MD-01-306, Department of Computer Science, University of Skövde, august 2001.