Information Security in a Heterogeneous Healthcare Domain

Rose-Mharie Åhlfeldt

School of Humanities and Informatics
University of Skövde
P.O. Box 408, S-541 28 Skövde
SWEDEN
rose-mharie.ahlfeldt@his.se

1 Background

Healthcare is an information-intensive activity involving the collection, communication and display of large amounts of information. This information is highly sensitive and most countries have special legislation to prevent its misuse. Hence, it is natural to use the support of computers in order to efficiently improve such an information-intensive organization. The increased use of computers for handling the information also gives access to information held in databases in a way that was previously impossible [21]. Swedish healthcare has gone through an efficiency improvement the last few years but it will also face major challenges and changes in the years to come.

With a new holistic view on the care offer and with a totally unbroken care-chain from the emergency treatment and primary care to rehabilitation and home healthcare and home services of the municipalities, new ways of working and new technology solutions are required. To decrease both time of care and waiting-time, and to increase the quality of the care, the information must be available for the care performers who need it, as quickly as possible, no matter where they are in the care-chain. One condition is that the information is current and correct, which is not always the case when the flood of information in the care stream is without computer support [23].

The main thing is to achieve two important aims concerning information security in healthcare. The first is to reach a high level of patient security, i.e. to give patients opportunities to the best care with right information in right time. The other aim is to reach a high level of patient privacy; i.e. to protect patients from that sensitive information is distributed to unauthorized persons. These aims are hard to reach together. Often this occurs at the expense of either one or the other aim. For that reason a balance between these aims is necessary when the work of information security within healthcare will be discussed [24].

This paper is divided in two parts. The first will give a background to the area of information security in healthcare and problems related to it. The second part will discuss the research problem area and address some research questions.

1.1 The patient record

One of the most central units in care information is the patient record. The traditional paper-based patient record used in a clinical setting generally contains the notes of clinicians and other care providers. Dahlin and Arnesjö [5] declare that the overall purpose of the patient record is to facilitate and support that the patient will be given excellent and secure care. This purpose presumes that record data is reliable and available when needed in the care and understandable for the care performers.

In the healthcare domain, there exist a large number of computerized patient records, so called electronical medical records (EMR). Many of them are single system and do not have the possibility to interact with each other. Just in one hospital there can exist hundreds of different EMR systems. These systems are autonomous and they have different purposes and functions for different kinds of businesses in healthcare. There are problems to exchange information between these systems within the same organization. The problems will not decrease when patient information is needed between different healthcare organizations, as well as primary care to municipalities or municipalities to hospitals or vice versa.

Since the EMR systems include sensitive patient information, the security aspects concerning the managing of these systems are very important. It is not just a piece of paper to take care of. The information is stored digitalized and is included in different systems. From a user's perspective, this can be hard to survey and control. New qualifications in the healthcare domain are required to manage the information security in a sufficient way [24].

1.2 Information Security

It is out of the scope of this paper to give an exact definition of the large number of security terms that exist in the literature. However, since the term information security is used in the paper, it is important do define what the term stands for. Information security is a broad term covering security issues in all kinds of information processing. It includes both technical and administrative security (Figure 1). According to SIS [9] information security is defined as security concerning information assets regarding ability to maintain a desired confidentiality, integrity and availability (also accountability and non repudiation are included). SITHS [17] defines the term information security as the collected effect of measures to minimize the risks addressed for the availability, confidentiality, integrity and accountability of information. In a computerized environment it is easy to focus more on technical measures and functions. It has still been shown that in order to get a sufficient level of information security in the organizations, a structured way of working is required both in planning and implementation of the security work. Furthermore, this is also important for the specific user in its daily work. If not the administrative security is function properly, the technical security will fall short for the security work at whole.

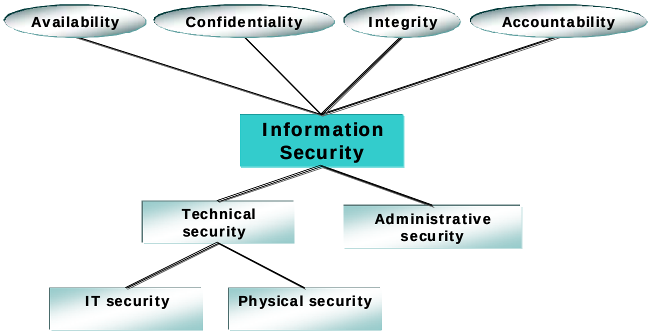

Fig. 1. Information Security Model

Information systems in healthcare are important systems for the society and information security in healthcare is therefore an important element to take into account. Most of the security problems are generic and concerns information systems in general. The Swedish Emergency Management Agency (SEMA) has in their report [16] pointed out some important conclusions concerning all important information systems in the Swedish society.

- Lack of a comprehensive view in information security
- There is a need of a base level of security in important society systems
- Internet should be classified as a critical infrastructure
- There is a need of a political comprehensive view concerning risks, crimes and threats related to information security
- The main threats are unintentional threats
- There is a great need of qualified education

These conclusions are generic for information security in the Swedish society, which imply that the healthcare sector also has to be brought up against with these problems.

Healthcare has a challenging task to deal with an increasing number of citizens, getting both older and sicker [3]. There are reports, showing that if the society is going to succeed with the future's need of care and with limited resources available, there is a need of effectiveness with IT as a support. The healthcare business claims that IT-support is necessary to preserve and improve service, availability and quality in care they are responsible for [3]. Therefore, to keep and improve information security in healthcare is a challenging task. According to SEMA [16] the need of research and studies in this area is obvious.

In the following sections, a number of current problems will be described more in detail. These problems are produced from earlier work and projects along with literature surveys. The describing problems are then going to be the base for the chose of my research problem and the continuing research studies in the area.

1.3 The integration problem

When IT-systems are going to be integrated, and when different healthcare organizations are going to share information with each other, it also makes new demands on information security. Not only the own organization must have a satisfying protection. Instead, the security boundaries are going to expand and the availability to sensitive information is increased. It makes new and bigger demands on security concerning networks, patients' privacy, access control systems etc. Furthermore, the administrative security gets further elements to take into consideration. Co-operated healthcare organizations' working processes and routines must also be considered.

Many healthcare organizations consider that the most important healthcare processes are the patient process [17]. This is the process that from the patient's perspective implies that different healthcare performers must co-operate together with the patient to increase the patient's quality of life. There is a need of a holistic view of information security and cooperative infrastructure for information security but also needs of techniques concerning strong authentication as well as the derived services as authorization, access controls, accountability, confidentiality etc. The SITHS project has created an infrastructure and model to meet all the demands mentioned above. Despite that, the healthcare organizations have not yet adopted this. Instead, they have still a long way to go. One of the reasons for the delay is limited economical resources. The projects also show that there is a need for further studies and research in this area [3].

The demands, mentioned above, are not unique for Swedish healthcare compared with other countries. Even if tradition and legal aspects are different between countries, the main problem is the same. Strong authentications, derived services as authorisation, access controls, accountability, integrity and confidentiality are importunate demands to provide [1], [2], [4,], [26].

When healthcare systems are going to be integrated the interest of a process oriented approach for healthcare information systems is increased [15]. Here, not only the technical and organizational demands on security are increased. Also, the patient privacy is important to keep protected when the patient processes will be extended in distributed systems including sensitive information. Louwerse [12] proclaims that with distributed systems in healthcare we need better awareness, better procedures, better software, and a more centralised approach or systems management.

One way for the healthcare units to be process oriented and integrated with other units' processes and IT systems is to introduce a process manager, which visualises and executes the communication between different IT systems; realised by using graphical and executable process models. The process manager also communicates directly with the healthcare personnel via desktop computers and mobile devices. VITA Nova [14] was a Swedish project which introduced a prototype system for healthcare processes based on a process manager. The result shows e.g. when introducing a process manager in healthcare it requires ways to deal with security issues (security, ethics, and legality). The healthcare units also show large differences in security awareness and IT maturity.

Transferring information between organizations must be done by designing solutions that are satisfactory from the perspectives of the patient and the patient's relatives as well as from a legal perspective. If healthcare in the future will be able to integrate its business processes with those of other care providers, and if transfer of patient information will be satisfactorily performed from a security perspective, routines for the minimum level of security have to be designed, documented and implemented jointly by all involved units [14].

1.4 The lack of security awareness and education

Ever since IT made its entrance to the healthcare sector, the lack of education has been more and more obvious. It's not only lack of education in the security area. Also education concerning teaching new information systems irrespective of their intentions for patient information, administration or network systems has been conspicuous by one's absence. Earlier work has shown that the users only got a few days to learn the system [29]. Depending on the minimum of time scheduled for education of new IT systems, there is neither space to keep up with nor any change to give priority to security education. This lead to users of IT systems in healthcare not having any adequate security education and this also implies that there are lacks of users' security awareness [6].

In the third report the SITHS project declares that the most important element to get the information security to work in an optimal way is education [18]. It is in the education existing threats, risks and possibilities can be pointed out. The SITHS proclaims that this is the way to build security awareness. Measures of security, no matter how technically advanced they are, can never replace the knowledge of the staff and the attitude to the security work. Furthermore, it is enormously important that ethics and moral is kept on a high level. The healthcare process rests on an information flow where the security solutions are needed all the time [18].

It is not only the users and workers in the healthcare sector who need education. Also the healthcare management needs education in information security. Katsikas [11] claim that "the most important pillar upon which any serious effort towards introducing and enforcing security in health information systems is based, is the level of awareness that those responsible for managing the effort have. Thus, the issue of proper awareness, training or education of healthcare management is of paramount importance". Different authors claim that education in information security is an important element, not only for users. Also the healthcare management need education in information security ([17], [18], [11], [29].

The lack of education is often related to the absence of established IT-security strategies and policy issues. Established IT-strategies or information security policies are not so common for the healthcare organisations nowadays [8], [7], [29]. This is an on-going work in the county councils and regions in Sweden. Some have accomplished more than others. Municipalities have the same situation but with bigger variations. There are municipalities with established strategies and policies whereas other municipalities just have started up with the work. According to SWEDAC [22], accredited organizations, for instance laboratories, have been forced to establish these documents which imply that the security work is satisfied and users' education in security issues is an on-going process. Furthermore, this situation has increased the users' security awareness on the whole, not just when they work with computerized systems. This will be in accordance to the result from the VITA Nova project [27]. There is a variation between the different healthcare units depending on how far the organizations have got in their establishing of security policies. The accredited organizations which have demands on themselves to establish security policies states that the employees have a much better security awareness than those organizations which have not come so far yet [14].

Even if strategies and policies are established, it happens that they are inconsistent. This is related to the own organization with different areas and different departments but also when patient information is going to be exchanged over different organisation boundaries. Inconsistent policies and procedures can lead to frustration, confusion and potentially even harm to patients. This is exemplified by differences in organisations' policy towards transmission of patient information by, for instance, facsimile. An organisation attempting to apply more restricted use of data transmissions is faced with complaints from other organisations with more lenient policies whose staff are frustrated that they can not send or receive patient information by that means [7].

The lack of a structured way of working according to information security is obvious in healthcare. There are just not only need for strategies and polices. Also following-up routines and routines for educational programs, evaluation of the strategies and policies etc. are needed.

1.5 Access profile levels

The access profiles are the parts of the access control system where different actors are defined and how they are allowed to process the information. In the existing access control systems there are differences concerning how sophisticated profiles they may create. To maintain a suitable level of information security for patient information, two models are most often combined; the authority model and the logging model.

Depending on the intensity of administration the authority model is required, the most system use the logging model in Swedish healthcare today. According to the SITHS-group, it is important for this kind of method that systems and administration to follow-up the logs exist [18]. There are differences between different care organizations how much resources can be reserved for administration in the models respectively. In most cases, one of the models is given priority to the expense of the other, according to [18]. Some care organizations can have clearly prepared and individually adapted access profiles, which take a lot of time to administrate at the same time as the following-up routines for the log is maintained to a limited extent. Other organizations have very “wide meshed” access profiles instead, which take less time to administrate. Instead, the greater part of the resources is reserved for following-up the logs [18].

Earlier work has shown that if not clear regulations exist and describing how the logs should be managed, there is a main risk that the logs are not checked at all. This implies that the trust for handling of patient information in healthcare can be called in question [10], [29].

Different authors claim that healthcare organizations should emphasize the authority model or “need to know principle” instead of the logging model or “right to know principle”. Gaunt [6] and Smith and Eloff [20], claim that the principal aim is to develop and implement need-to-know authority-controls that would protect patients’ healthcare data. The user would only be allowed to access information necessary to complete his or her job.

Irrespective of what kind of levels of access profiles are used, it is essential to examine the consequences of the choice of levels for the organizations. Since the authority model emphasize the patient’s integrity, the logging model straight forward the need of efficiency of the business and put one’s confidence in the user’s ethics. According to earlier works, mentioned above [19], it is important to find a combination between these two models since the aim is always to reach a balance between the patient’s integrity and the efficiency of the care.

If an authority control should be worked effectively, the trust of the user’s identity must be required. The user must be the person she/he says she/he is. Technically, this can be an easy task to provide when users use own computers at their working places. However, in healthcare there are limited resources also concerning computer equipments and therefore it is common that users use the same computer to perform their tasks. Earlier work has shown that instead of taking time for log-in and log-out procedures, the users use each others’ passwords and perform searches of patient information in someone else’s user’s session [30]. This can lead to crime since secrecy is not covered, or the opposite, authorized information access gives judgments when the logs are checked.

2 Research plan

2.1 The research problem

The problems mentioned above are by no means the only ones in the healthcare area. However, these problems are frequently returned in studies and interviews with involved actors. Both the educational problem and the problem with access profile levels are important issues separately and could be a research problem for research investigation on their own. In my research I will concentrate on further examining security issues related to the integration problem. However, this will not exclude dealing with the other two problems.

The integration problem has been chosen due to the fact that both practice and research has pointed out the necessity of finding safe and sound solutions to the integration of patient information systems within and among the business processes in which they are involved. Information provision in healthcare must be effective such as to contribute to giving patients the care they need. Hence, information security related to business and systems integration is an important issue in particular for maintaining the citizens' trust for healthcare.

In order to come to grips with this problem it needs first of all to be well understood, i.e. we need to make an in-depth study of information security needs including the current state of the art in healthcare processes, in particular where more than one healthcare provider is involved. As a prerequisite to this we need also to find out and analyse what kinds of statutes and regulations that may have an impact on possible solutions. For the research to be useful one needs finally to complement existing business and systems development methodology with useful advice and guidelines for how to reach a satisfactory level of information security.

In accordance with this discussion, a number of research questions may be formulated:

- *What are the information security problems experienced in current heterogeneous healthcare processes?*
- *What are the needs and requirements for information security in healthcare when different healthcare performers integrate their business processes with included patient information?*
- *How do we need to complement business and systems development methodology in order for it to provide adequate support to building solutions with a satisfactory level of information security in healthcare?*

Figure 2 shows in what way the two first questions are related to each other. They are at the same level and are very much connected. When a problem is encountered, it will bring up new needs and requirements, but also when new needs and requirements are discovered, new problems will arise. It is necessary to make a number of iterations in order to give the survey an adequate scope. The results from the first two questions will then be used to build solutions to complement current methodologies.

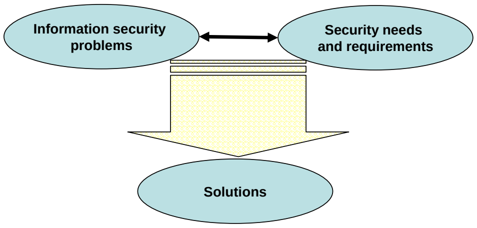
Information security problems
Security needs and requirements
Solutions

Fig. 2.Research process outline

2.2 Research approach

Some activities in the process can be as follow:

1. A literature survey within the areas of information security, healthcare informatics and healthcare business process integration.
2. Studies of healthcare processes, their need for integration, current integration solutions and the problems caused by these.
3. Observations and interviews with involved actors in the healthcare business processes.
4. Structured interviews with patients involved in the healthcare integrated business processes.
5. Analyze and development work in order to design advice and guidelines as a complement to current business and systems development methodology.
6. Validation process of suggested solution in practice and focus groups with related healthcare actors.

Since I am involved in some on-going research projects in the healthcare area, both in Sweden and Europe, I will use the opportunity to perform healthcare process studies, observations and interviews in co-operation with these projects. In particular, the activities 2 – 3 are conducted within the research projects VITA Nova [27], VITA Nova Hemma [28] and MobiS@ms [13]. However, also other relevant healthcare actors than those engaged in those projects will be involved in the work.

Some work has already been done and below is a brief description of the results and their references.

- The literature survey is an on-going process and will be done in parallel to other work.
- Observations and interviews has been done in subprojects

  - MsC dissertation with focus on information security in home healthcare. The result from this work has been published in [29].
  - A study about information security in EMR with the user in focus. This study was carried out from a hospital point of view and the result is published in [30].
  - Study about system and network security in different heterogeneous healthcare performers. This is a case study in collaboration with the VITA Nova project. The result shall be presented and published at the Security Conference in Las Vegas, March 2005 [31].
  - A study at how a process oriented systems architecture can be used in healthcare. The result has been published in the Healthcare Informatics Journal [25].
  - An experience report about how a process manager can be introduced in the healthcare business processes. The result has been published in [14].
- The structured interviews are an on-going process in collaboration with the MobiS@ms project and will be finished in June 2005.

The result from the activities 1-4 will form the basis for a PhLic[1] dissertation concerning state of the art and state of practice of information security in integrated business processes in healthcare. The results from the activities 5-6 will then be added to the PhD dissertation.

3 Conclusion

Information security has an important position in the healthcare’s information processes. This is not a new thing and plenty of work has been done in this area both in Sweden and other countries. There is still not so much done in the research area about the aspects of information security when different healthcare performers would interoperate their business processes with each other in an efficient way. A research work like this should then be urgent both for the research community and the healthcare domain with respect to their trustworthiness and to find a sufficient level between patient security and patient privacy over the patient care process.

References

1. Blobel, B., (1997) Security Requirements and Solutions in Distributed Electronic Health Records. Computers and Security, 16, pp. 208-209.
2. Blobel, B. and Roger-France, F., (2001). A systematic apporach for analysis and design of secure health information systems. International Journal of Medical Informatics 62, pp. 51-78.

[1] Licenciate of Philosophy – in Sweden a half way graduation to a PhD.

3. Carelink (2003). New agreement for SITHS-CA [on-line]. Available from: http://www.carelink.se [Accessed 3 January 2003].
4. CEN TC 251, prENV 13729: Health Inormatics Secure User Identification - Strong Authentication using Microprocessor Cards (SEC-ID/CARDS), (1999).
5. Dahlin, B. and Arnesjö, B. (1996). Datorjournalen. In: G. Petersson and m. Rydmark, editors Medicinsk Informatik. Liber Utbildning, chapter 6 (in Swedish).
6. Gaunt, N. (1998). Installing an appropriate information security policy. Internation Journal of Medical Informatics, 49, pp. 131-134.
7. Gaunt, N. (2000). Practical approaches to create a security culture. International Journal of Medical Informatics, 60, pp. 151-157.
8. Gritzalis, D. (1997) A baseline security policy for distributed healthcare information system. Computer & Security Vol 16, No 8, pp. 709-719.
9. SIS (2003). SIS Handbok 550. Terminologi för Informationssäkerhet. Stockholm 2003 (in Swedish).
10. Karlsson, K., (2003). Right-to-know inom hälso och sjukvården. Msc thesis, Department of Computer and Systems Sciences. Stockholm, Stockholm University & Royal Institute of Technology. Available from: http://www.simovits.com/arhcive/CatKarl.pdf [Accessed 2 April 2003] (in Swedish).
11. Katsikas, S. K. (2000). Healthcare management and information system security: awarnesss, training or education? International Journal of Medical Informatics, 60, pp.: 129-135.
12. Louwerse, K. (1998). Availability of health data; reguirements and solutions Chairpersons' introduction. International of Medical Informatics, 49, pp. 9-11.
13. MobiS@ms (2003). Projektplan Mobis@ms [online] http://www.lime.ki.se/mobisams. [Accessed Jan 2005] (in Swedish).
14. Perjons, E., Wangler, B., Wäyrynen, J. and Åhlfeldt, R-M. (2004). Introducing a Process Manager in Healthcare: An experience report. In Proceedings of the Ninth International Symposium on Health Information Management Research (iSHiMR), Sheffield, June 15-17, 2004, pp. 71-86.
15. Poulymenopoulou, M., Malamateniou, F. and Vassilacopoulos, G., (2003) Specifying Workflow Process Requirements for an Emergency Medical Service. Journal of Medical Systems, 27(4), pp. 325-335.
16. SEMA (1999). FA22. Swedish Emergency Management Agency. Växjö, Grafiska Punkten. 3 (in Swedish).
17. SITHS-projekt, (1999). Informationssäkerhet i vårdprocessen: Krav beskrivna i generella användningsfall utifrån vårdcenarion, Stockholm: Säker IT i Hälso- och sjukvården, ISBN 91-7188-565-X (in Swedish).
18. SITHS-projekt, (2000a). Tjänster för att uppnå informationssäkerhet i hälso- och sjukvården. Stockholm: Säker IT i Hälso och Sjukvården, ISBN 92-7188-607-9 (in Swedish).
19. SITHS-projekt, (2000b). Infrastruktur för informationssäkerhet i hälso- och sjukvården. Stockholm: Säker IT i Hälso- och Sjukvården, ISBN 92- (in Swedish).
20. Smith, E. and Eloff, J. H. P. (1999). "Security in healthcare information systems - current trends." Internation Journal of Medical Informatics 54: 39-54.
21. Spri (1996). Behörighet, säkerhet och sekretess - krav på system med patientinformation. Spri rapport 419. Stockholm, Spri (in Swedish).
22. SWEDAC (2003). SWEDAC:s föreskrifter STAFS 2003:13. [on-line] http://www.swedac.se [Accessed May 2004] (in Swedish).
23. Sågänger, J. and Utbult, M. (1998). Vårdkedjan och informationstekniken, Teldok. (in Swedish)

24 Teldok (2004). Patientdata - brist och överflöd i vården. Teldok rapport nr 154. ISSN 0281 - 8574 (in Swedish).

25. Wangler, B., Åhlfeldt, R. and Perjons, E., (2003) Process Oriented Information Systems Architectures in Healthcare. *Health Informatics Journal*, Vol 9(4), 253 - 265, December 2003

26. Wenzlaff, P., Blobel, B. and Pharow, P., (1999) Health Professinal Cards: awarenss for security in Health Care Networks, in: F. Sicurello (Ed.), Healthcards '99, XASI, Milan, 1999, pp 121-125.

27. VITA Nova, *(*2002). Projektplan VITA Nova I [online]. http://www.ida.his.se/ida/research/vitanova [Accessed Jan 2005] (in Swedish).

28. VITA Nova Hemma, *(*2003). Projektplan VITA Nova Hemma, [online]. http://www.ida.his.se/ida/research/vitanova [Accessed Jan 2005] (in Swedish).

29. Åhlfeldt, R.-M. (2002). Information Security in Home Healthcare; A case study. In the Conference Proceedings of the Third International Conference of the Australian Institute of Computer Ethics (AiCE) 2002. Sydney, Australia, 30 September 2002, pp. 1-10. Eds. M. Warren and J. Barlow. Australian Institute of Computer Ethics.

30. Åhlfeldt, R-M. and Ask, L. (2004). Information Security in Electronic Medical Records: A case study with the user in focus. In Proceedings of the 2004 Information Resources Management Association International Conference. New Orleans, USA, May, pp. 345-347.

31. Åhlfeldt, R-M. and Nohlberg, M. (2005). System and Network Security in a Heterogenous Healthcare Domain: A Case Study. In Proceedings of the 2005 Security Conference, Las Vegas, USA, Mars, to be appered.