Växjö University

School of Mathematics and Systems Engineering

Reports from MSI - Rapporter från MSI

Protect Data Privacy in E-Healthcare in Sweden

Nan An

Sep
2007

MSI
Växjö University
SE-351 95 VÄXJÖ

Report 07114
ISSN 1650-2647
ISRN VXU/MSI/IV/E/--07114/--SE

Abstract

Sweden healthcare adopted much ICT (information and communication technology). It is a highly information intensive place. This thesis gives a brief description of the background of healthcare in Sweden and ICT adoption in healthcare, introduces an Information system security model, describes the technology and law about data privacy and carries out a case through questionnaire and interview.

Acknowledgement

Here I would like to say thank you to all those people who has help me during the process of the thesis. First I have to thank Linda Askenas, my supervisor. She gives me a lot of advices and help with the interview. Second I should thank Kaj.Stenkilsson, the man who is in the field of information security in Växjö University. He taught me a lot about information security. Thirdly I appreciate the library of Växjö University. The workers in the library offering me selfless help for the English version of Swedish law/acts about data privacy in e-healthcare. Then I would like to thank David.Nadel, the teacher of database in Växjö University. He gave me many articles about information security in Sweden while I cannot find much in the beginning. Moreover, I want to thank Yuan Wang and Xiang Zhang, my classmates. They enlighten me a lot about the content and the structure of the thesis. Finally I want to thank for all the security man in the regional hospital that give me help with the questionnaire. They spare their leisure time to do the questionnaire for me. If not for all the people above, I would not finish the thesis. I really thank you all!

Key words:
Data privacy, health care, Sweden

Content

Index of figures/tables:

A

E

F

T

Chapter1

In this chapter, an introduction of whole thesis is presented. The background of Sweden health care is briefly described. The ICT (information and communication technology) adopted in health care in Sweden is also illustrated. After this, I explain why I decided to write about this field. Then the process of formulation of the topic is listed and described in detail.

What are data privacy and the relation between security and privacy are included in "1.5 subject area". If you have any questions about the glossary in the thesis, please always remember to check if it is in "1.5.3 Data privacy related glossary/abbreviations".

Who are the audience of the thesis? Chapter 1.6 gives out the scope of audiences and potential audiences.

Chapter 1.7 tells the limitation of the thesis.

1.1 Introduction

As long as the popularity of patient records to be transferred electronically and the wide use of World Wide Web, the problem of protecting data privacy gradually arises.

Sweden is a country utilize Information and Communication Technology much in healthcare, nearly every branches of healthcare has the information system. The information is transported through the internet very quickly. This convenience is a double blade sword.

On one hand, it reduces the error of patient to take the handwritten encryption to the pharmacy for the medicine. It save the time and money spend on maintain the paper document of patient. The therapist could get access to the appropriate Electronic Patient Record when needed. One the other hand, the jeopardy of abuse of personal data is increasing. Encroachment of personal data has become more and more common. Privacy-invasive technology has been developing. The most dangerous type of attack is the Re-identification method. In this way, even the anonymous personal

data are vulnerable. Fortunately, the de-identification method is developing too. The technique related to de-identification method are introduced in 2.2.2.

Except for the threat produced by outsiders, the threat produced by the authorized people is also dangerous or even more dangerous. The introduction of authorized people abuse personal data is introduced in 1.3 and 2.3.

For protecting patient away from insider abuse of personal data, acts are listed and interpreted in 2.3. All the laws and acts related to patient data privacy from the universal level to Sweden level.

This thesis is in the scale of master thesis. It carries out the case about data privacy. What approaches toward data privacy is studied here. A questionnaire is sent to security man of each regional company. The case is based on the answer from the security men. After careful analysis of the results, a conclusion will be given out.

This thesis aims to give some primary knowledge of data privacy and information security to average people. More emphasis will be given on the law and ethic part.

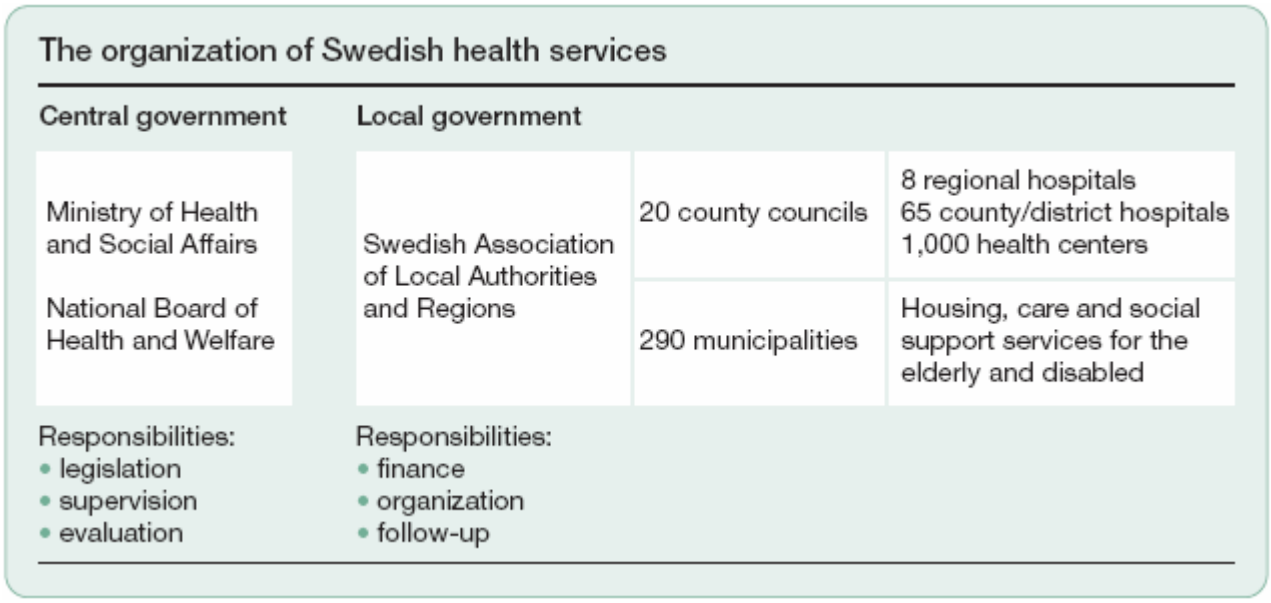
1.2 Background

1.2.1Background of Sweden Health care

A brief introduction to Swedish health care:
9,117,712(2007-January, Statistics Sweden) people in Sweden have the same access to the health care. One word could describe this national owned and funded system could be "decentralized". Without much cost restriction, the system is success compared to other countries at a similar development level.

Why the system described as "decentralized"? It is because the management of it. The duty for providing health care is held by the county councils and sometimes the municipalities. the county council is not appointed by the government but elected every four years on the same day as the national general election. Providing good-quality health services and medical care as well as aiming at improving health in the whole nation are the policy of every county council.

20 county councils and one municipality (island of Gotland) are in charge of the health care. 290 municipalities provide care for elderly people, including the physical or psychological disabilities. These municipalities don't provide service of doctors.



The organization of Swedish health services

Central government	Local government		
Ministry of Health and Social Affairs National Board of Health and Welfare	Swedish Association of Local Authorities and Regions	20 county councils	8 regional hospitals 65 county/district hospitals 1,000 health centers
		290 municipalities	Housing, care and social support services for the elderly and disabled
Responsibilities: • legislation • supervision • evaluation	Responsibilities: • finance • organization • follow-up		

(Fact sheet, "Swedish health care", 2007)

Figure1 the organization of Swedish health service [Szolovits, "Patient Data Privacy in Electronic Records"]

Cooperating with the Swedish Association of Local Authorities and Regions, central government establishes the principles, guidelines and political agenda for health and medical care.

Primary care (abbreviation 2) is made to be the foundation for the health care system although it is not considered so important in the past. In health care centers, patients should be able to choose their own doctors. 25% health centers are private. County councils commission the enterprise that runs the private health centers.

Where is the capital for health care coming from? It comes mainly from three parts. They are local taxation (71%), contribution from the state (16%), and patient fee (3%). the remaining 10% comes from other contributions, sales and other sources. The cost for health and medical care takes nearly 9% of Sweden's gross domestic product.

Now it is common for county councils to buy health services. 10% of health care is financed by county councils but carried out by private health care providers. This adds

to the accessibility of health service.

The fee patient has to pay is listed in the table below:

The system could be better if not for long waiting times for pre-planned care. To solve this problem, a care guarantee is established by the central government and the county councils in 2005. If what the care needed is decided, the guarantee ensures that patient could get access to the health care he/she needs within 3 months. For expiration of waiting time, other place will take charge of the patient and the fee is paid by his/her own county council.

In the future, the chance for everyone to get access to the integrated health care would increase. The health service will be offered from hospitals, health centers and social services.

Kinds of health service	**Fee**	High-cost ceiling: After the patient has paid a total of SEK 900, medical consultations in the 12 months following are free. For prescribed medication there is the same ceiling **No one pays more than SEK 1,800 per 12 month period**
Staying in a hospital a day	80	
Consult a primary care physician	100-150	
Make an appointment with a specialist	More than consult primary care physician	

Table 2 fee of health service

As we have said before, the obvious characteristic of Swedish health care is "decentralized". Each county council is founded mostly by the local taxation (71%) and run by its own. the national data is not enough.

"However, there will soon be an improvement here because the National Board of Health and Welfare and the Swedish Association of Local Authorities and Regions have agreed to establish a model for comparing and evaluating achieved goals and

results.

There are many reasons for this:

• To provide a better platform for public debate and political decisions,

• To make it easier for county councils and municipalities to manage and streamline Health care and

• To provide the general population and patients with more easily accessible information.

Statistics based on national research have already been produced on issues such as Health effects, quality, patient security, waiting times, patient opinions and costs. This type of benchmarking enables county councils to be evaluated in relation to each other." (Fact sheet, 2007)

1.2.2 ICT adoption in Sweden Health care

The tendency of health care in Sweden

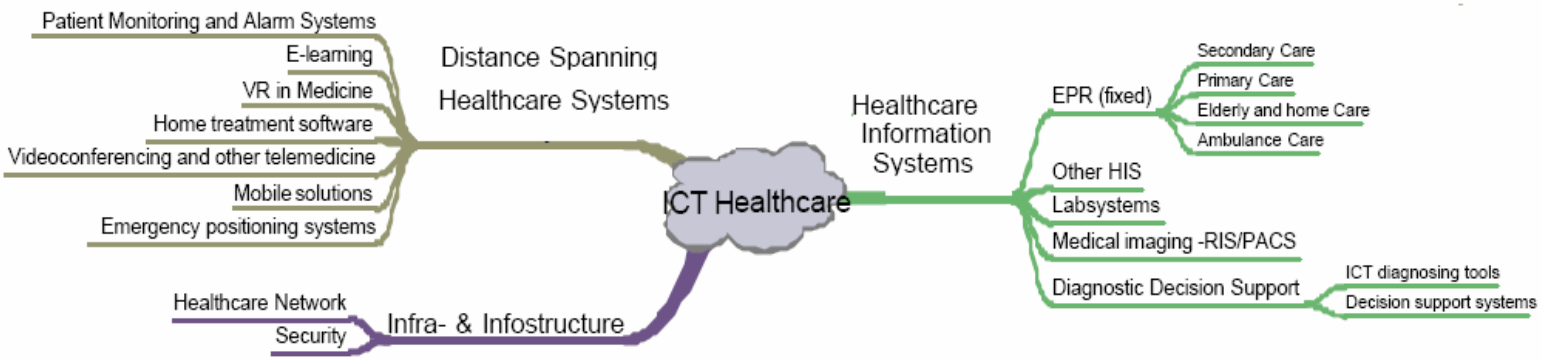
Before we talk about the tendency of health care in Sweden, the definition of ICT should be introduced firstly.

"IT, as defined by the Information Technology Association of America (ITAA)is: 'the study, design, development, implementation, support or management of computer-based information systems, particularly software applications and computer hardware.' In short, IT deals with the use of electronic computers and computer software to convert, store, protect, process, transmit and retrieve information."-[Wikipedia]

By adding the concept of electronic communication into IT, IT is broadened as ICT---the Information and Communication technology.

ICT is widely used in the Swedish health care.

Figure2 ICT health care in Sweden Tarre, "Applied ICT in the Healthcare industry in Sweden-A study conducted by Kristina Tarre on behalf of Invest in Sweden Agency's IT Sweden Project"



The Swedish Healthcare ICT costs 2002 are approximately 3.84% of turnover in health care. The ICT used in different department increase the efficiency, decrease the cost. The high invest in ICT of health care makes big contribution to Swedish's ranking Second in the international health cares although Sweden has so many elderly people.

In 2003, more than 95% of Swedish primary health care adopted EPR. More than 20% prescriptions are electronic prescriptions. Over 50% of the radiology departments are digitalized. 30-35% hospitals have implemented an EPR. "There is probably no country that has come as far as Sweden in terms of general overall implementation of ICT in the healthcare services"[Tarre, 2003, p.23]

Let us see the regional analysis of health care (figure3):

The use of ICT permeates into the health care very deep. The information flow in the health care is highly electronic. That is one reason for why the data privacy is necessary.

Because the elderly people in Sweden will increase. As analyzed, 24,000 doctors will be recruited in the next ten years. The utilization of ICT will support the remote health care, in order to solve the problem of lack of doctor, specialist. As a consequence, the government is seeking for more efforts on this part, although Sweden has been successful with the implementation of ICT in the health care so far. In 2002, a report "VårdITiden – strategier och åtgärder för att bredda användningen

av telemedicin och distansöverbryggande vård"[2002] is presented. VardITiden mentioned that "An IT security solution with the fundamental security functions for identification, electronic signature and encryption"[VardITiden, 2002] is needed for further implementation of IT in the health care services.

	Linköping/ Norrköping - ESDA	**Västerbotten/ Norrbotten – Internetbay**	**Gothenburg - BRG and Västra-götaland**	**Stockholm/ Kista – Mobile Valley**	**Blekinge – Telecom City**	**Skåne – Postion Skåne**
Regional strengths	Medical imaging Sensors on body VR in medicine Vårdinforma-tionsnätet	Implementa-tion of ICT Telemedicine Home Healthcare Sensors on body VR in medicine Tillit	VR in medicine Patient Monitoring Systems	Home healthcare VR in medicine Telemedicine Medical Imaging Patient Monitoring	OVK – information in the chain of care Mobile applications for home and elderly care	Medical imaging VR medicine Merging bioinformatics with health-care
Implement. ICT in operations						
EPR	++	+++	+	+	++	++
Digital radiology	++	++	+	++	+	+++
E-prescription	+	+++	-	-	+++	+
Telemedicine	++	+++	+	++	-	++
Competence						
Telemedicine	++	+++	++	++	+	++
Medical Imaging	+++	++	++	++	+	++
Virtual reality	++	++	++	+	-	-
ICT in elderly and home healthcare	++	+++	++	+++	++	++
ICT supporting the chain of care	+++	+++	+	+	+++	+++
Education	+++	++	++	+++	-	+

Figure 3 regional analysis of health care [Tarre, 2003, p.19]

+++ = very strong

++ = strong

+ = some strength

- = insignificant

As far as I know, "The French IT consultancy company Steria is one of the major players in security solutions." [Tarre, 2003, p.10] But in the following six regions, only Stockholm/Kista adopts the Steria. The six regions are 1, Linköping/Norrköping, 2.Norrbotten/Västerbotten, 3.Skåne, 4.Gothenburg, 5.Blekinge, 6.Stockholm/Kista. I don't know what kind of approach the other regional hospital use towards data privacy and if they are enough for protecting the patients' privacy. Thus I think start to study the approaches they have would give us some hint towards how to improve the data privacy.

1.3 Motivation

Generally speaking, to write this topic is both out of the importance of data privacy in healthcare and my personal interest.

With the dramatic growing of usage of World Wide Web, more and more documents are transferred into electronic documents. It provides both convenience for use and chance for criminal to commit crime. The storage and transporting of paper based document are very inconvenient for the big volume and fragility of paper document. The information system and digital document solve these problems. Millions of records could be stored in a small disk or be transmitted to another place in a flash. However, it is almost impossible for someone to break into the house to steal pile of paper document but it is easier for someone to break into the information system and attack the system.

Let us take three examples:
1. When five American Veterans organizations decided to sue Veterans Affairs of lost of 26500,000 identity data, the Federal government admitted that this issue does not only affect the veterans, but also affect 80% soldiers now. This issue was caused by an employee taking a hard disk which contains millions identities of veterans and soldiers in commission now. Someone steals this hard-disk in the night.

2.Washington University medical center announced that some hack invade the database and steal partial patient record and medical information, including name, health status, home address, social security number and therapy approach.

The medical center said the hack get access to the password of the medical center on a public net. Then he pretended to be the legal user and steal information of more than 4000 patients.

This issue causes worry of related professional about network security of medical system. Experiencing this, the speed of hospital to adopt network would be affected to some extend.

3. An investigation is made by Statistic Sweden about how many people's information security is encroached: (this tale is the people whose information is abused during the period April 2004-March 2005)

age	Proportion in percent					
	total	female	male	total	female	male
16-24	5	5	6	56,718	25,866	30,852
25-34	5	4	6	56,998	25,278	31,720
35-44	4	3	5	52,650	20,880	31,770
45-54	2	2	3	25,108	10,074	15,035
55-74	1	1	2	28,613	10,316	18,297

Table 1 [statistic Sweden, http://w41.scb.se/templates/tableOrChart____154531.asp, Tabell 91]

The above three examples show the necessity of information security. It also shows the necessity of protecting data privacy through increasing information security. These issues motivate me to write something about data privacy in e-health care in Sweden.

At the same time, I myself am very interested in the security issue when I was taking the course "Participative Thinking". Then I wrote a report about the train ticket sites. I found that there seems to be no obvious approach towards security with the payment by credit card online. That once made me suffering after I bought some train tickets online. I was too worried about the disclosure of my credit card number.

When I started my master thesis, I choose to study the data privacy. But take the data privacy as the topic is too broad. As a consequence, I decided to narrow down the topic. After check the definition of the data privacy, I found out that health

information is one of the most common data affected by data privacy. Moreover, Sweden is famous for its health care system all over the world. There would be a bulk of things to discuss. The topic would be very interesting and full of challenge.

1.4 Topic formulation

How the topic is formed?
The original question is “how to improve the data privacy in e-healthcare in Sweden?”

The research rationale: Sweden is a developed country. People here enjoy high social welfare. The health care is one of them. Because of careful management and high ICT utilization in health service, Sweden ranks high in international heath care. Everyone get equal access to the health care.

But problem exist in two ways:
1. People are not aware of the importance of the data privacy in health care.
2. People care too much of the data security of health care, the researchers cannot carry out the study properly because they have to ask for permission before use the data.

This paper aims to help the first type of people. Not going too deep to the technical part, the simple comparison of existing approaches towards security in regional hospitals gives out the suggestion or solution for improving the data privacy. In the process, people of first kind as the audience could get more knowledge about the data privacy in healthcare.

Specifying questions:
What approaches does each regional hospital now use for data privacy?
How to generalize the advantage of each hospital?

1.5 Subject area

1.5.1 Definition

The thesis is mainly about the data privacy. First we gives out the brief concept about

the data privacy:

"Data privacy refers to the evolving relationship between technology and the legal right to, or public expectation of privacy in the collection and sharing of data."[Wikipedia]

"Loosely speaking, data privacy means the ability to protect selected information against selected parties."[Wright, 2005, p.1]

What is privacy?
“Privacy is the state of being free from intrusion, and in the context of health care it concerns the responsibility of a care provider to protect a patient from any disclosure (i.e., discovery by others), even unintentional, of personal health data, by providing security to the patient and the patient's records.”[Davis, 1999, p.1]

1.5.2 Security and privacy

The data privacy is always mentioned together with the data security. But people get confused easily when facing the concept of security and privacy. Security and privacy are related to each other but different in many aspects.

The privacy has a plethora of definitions. As well, the concept of security is rather broad. It contains aspects such as cyber-security, airport security and even national security. The mainly focus of security in this thesis is the information security---the control of illegal disclosure, unauthorized access, and use of information.

Security is on a higher level than the privacy. When passengers pass the custom, their luggage is checked to make sure that there is no dangerous stuff in it. High surveillance would invade the privacy of the passengers but protect the security of the airport. To protect the security of the system, the privacy of the user of the system would be sacrificed. Their action would be supervised under strict rules.

In most cases security and privacy are complementary to each other rather than controversial. Security is a tool for protecting privacy. No matter how perfect the privacy rule is, when hack breaks into the system they can't help. In a well designed

system, security is essential part for data privacy. "Both privacy and security share a complementary goal — stopping unauthorized access, use, and disclosure of personal information." [Swire, Steinfeld, 2002, p.4] Good security mechanism also creates audit trails about who has access what data in the system. As the owner of the personal data, the patient have right to know who has been seen his/her data. This decrease the chance that authorized user abuse their right--discloses or sells the patient data.

1.5.3 Data privacy related glossary/abbreviations

- ICT Information-Information and Communication technology

- confidentiality of personal information

"Confidentiality is privacy of content" [Thomas, Loader, 2000]

"In general usage, confidentiality of personal information protects the interests of the organization while privacy protects the autonomy of the individual; but, in medical usage, both terms often mean privacy." [Sweeney, 2001, p.35]

- integrity of personal information

Integrity of information confirms the accuracy of the information. That is to say, the information should be correct. Moreover, the data should be authentic enough for relying upon. That means the data shouldn't be changed during the transporting. Integrity is an paramount indicator of information security.

- Availability

Availability is the insurance for system to function properly. The access control list, authentication or the system would contribute to prevent unauthorized users to get access to the sensitive information. The availability means the authorized users would get access to the information when they needed. For example, a clinician being kept away by the system from access to the Electronic Patient Record is the sign of the system lack of availability.

- anonymity

"The term anonymous data implies that the data cannot be manipulated or linked to identify an individual"[Sweeney, "Computational Disclosure Control-A Primer on

Data Privacy Protection"]

"Anonymity is privacy of identity" [Thomas, Loader, 2000]

- data process

Processing of personal data includes, for example, collection, recording, storage, adaptation or alteration, compilation or retrieval. [Ministry of Justice of Sweden, "Information on the Personal Data Act", 1998, p.1]

- INFOSEC – short for Information System Security

1.6 Audience and potential audience

"The important fact is that not everybody is aware of the existence of surveillance, and even fewer people are familiar with privacy-protection methods. That is something which demands knowledge as well as engagement."**[Crnkovic G, 2006]**

For the majority of people, they will never hesitate to offer any information to their doctor or primary care consultant.

In the past, the most patient record is stored in paper form. It seldom happens that some one break into the physical wall and steal the record.

The government decides to make hospitals to store the patients' record permanently for "a full medical history is available for each patient, for future reference." [Global 360, "Customer Success Story: Akademiska Sjukhuset - Uppsala University Hospital"]With time pass by, there are more and more paper record stored. Take the Uppsala University Hospital as an example, "By 2003, some 600 million paper documents were still being stored in rented document storage facilities. These required 10km of shelf space, which was costing some 20 million Swedish Crowns (c. US $2.9m) a year in rental and costs for staff employed in these archives." [Global 360, "Customer Success Story: Akademiska Sjukhuset - Uppsala University Hospital"]

To solve this problem, Uppsala University hospital adopts the "Global 360 KoVIS system" to store the electronic patient record.

‘“From 2007, the Hospital will save some 3 million Swedish Crowns in storage facility rental charges. And in addition the Hospital will begin to save on staff costs: fewer administrative staff will be needed as records will no longer have to be manually located, retrieved, passed between departments or re-filed. So there will be more money to spend on direct health care and medical equipment and facilities’”. [Global 360, “Customer Success Story: Akademiska Sjukhuset - Uppsala University Hospital”]

From this example we could judge that the ICT utilization in health care is a main tendency in the future. The old paper records are scanned by special machine to be transformed into electronic form. The new records are born to be electronic.

This change just happened in several years. A large number of people are not ready for such change or not ready for the risk of the change. April 2004-March 2005

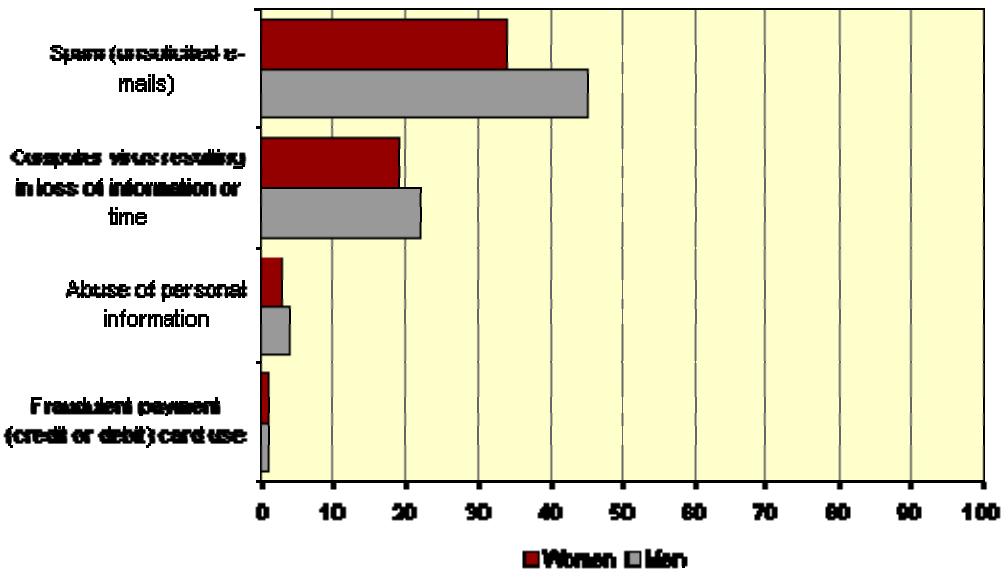


Figure 4 Proportion of persons aged 16-74 who have encountered different security problems when using the Internet, per cent [Statistic Sweden, http://w41.scb.se/templates/tableOrChart____154531.asp, 2007/April/25th]

April 2004-March 2005

Believe or not, the Web security in the commercial area is very serious today. Some insurance companies are warned by the Value Analysis（VA）data stolen. The

employees of these companies download the patient data on the laptop and bring it home for work. It is very hard to prohibit this kind of behavior, but the privacy should be protected anyway.

In such a highly electronic society, the chance for cyber-crime is big. Figure 4 gives out the profile of the condition. Although the percentage of personal information abuse is not very high, to the victim, the percentage is 100%. The disclosure and abuse of personal data would surely make the victim suffer. Trying to avoid such kind of issue before it happens is the best way.

From the informatics aspect, this thesis would not go too far in the technique way. Although some technologies are introduced, they are introduced in a simple way. The law will be paid more consideration. Nearly all citizens could get a simple introduction to the data privacy issue from this thesis, especially those ones who don't pay much attention to the data privacy before. Their knowledge towards this subject in health care area will be enhanced in some way.

1.7limitation

There are 8 regional hospitals, 65 county/district hospitals and 1,000 health centers in Sweden according to the fact sheet [2007, January]. If time and energy allowed, the more hospitals and health centers are investigated, the more general the result could be. Unfortunately, I just work alone. Moreover, as a foreign student who cannot speak Swedish, investigation at some district/county hospitals would be impossible. The aforementioned reason leads to the first limitation of my study-not many hospitals are included. However, the regional hospitals are big. They could be treated as representatives of the other small scaled hospitals and health centers. Some of them are very famous even internationally.

The second limitation of my thesis is that it doesn't concern much on the technical part. As an informatics student, I didn't learn how to make the system secure through the design of system. All I could do is to organize a questionnaire concern both the techniques and ethical/law part of the local hospitals. The advice for how to improve the data privacy in e-health care would be offered after the comparison. In this process, every definition would be interpreted in several aspects. Plain language would be

mainly used. Everyone could get to understand my work without academic background. In this way, I believe my study would make some contribution to the understanding of people about data privacy.

Chapter2

This chapter is a crucial part of the thesis. It consists of the research approach, models and data collection techniques.

How the thesis is structured totally depends on the research method. The information security model is explained briefly here to give a curtness of its meaning. The model would serve as a guideline for the analysis of the thesis.

2.2 illustrate the relation of the privacy and technology while 2.3 present the law and ethical view of data privacy. Which one is more important between technology and law, ethic? The audience would get a clearer view after reading these two parts.

2.1Method, Model and data collection

2.1.1 Method

The research will follow Jenkin's (1985) model of the research process contains 8 sequential steps.

1. Idea
2. Library research
3. Research topic
4. Research strategy
5. Experimental design
6. Data capture
7. Data analysis
8. Publish results

This thesis contains the normal way of study, the chosen of theory, methodology, and the input of empirical observation and the output of the conclusion.

2.1.2

Our work in this thesis is both based on literature and empirical work. According to Pertti, Jävinen ("ON RESEARCH METHODS", p.10), our work uses theory-testing approach because we use the model and theory to guide us in the process of study.

For data gathering, observation, interview and the questionnaire are used.

Survey is a very frequently used approach of research.. Acquiring documents is used in the thesis. Secondary source is used as acquiring documents. The background of Sweden Healthcare is from the Fact Sheet on http://www.sweden.se. The statistic about the information security status in Sweden is from http://www.scb.se/ (Statistic Sweden). These are all secondary sources.

Bell (1993, p. 93) recommended a formalized or structured interview. According to his list, we selected:
1) list what you need to know; 2) why you need this information; 3) is interview the best way of get the information?; 4) device question in outline; 5) decide the type of interview 6) select the person you would interview with; 8) make appointment. Bell has a long checking list, only several step are listed here as a guidance for the case study.

As mentioned in 1.2.2, approaches towards data privacy/information security are what the case needs. There are nine regional hospitals in Sweden. After the telephone interview and email, four answers are collected. Exactly speaking, the thesis uses a survey, not a case study. The questionnaire is not used as the traditional questionnaire. Normally the questionnaire is sent to be fulfilled by at least hundreds of people. The questionnaire is only used as a tool for collecting ideas from security man from different hospitals.

2.1.3 Information security Model

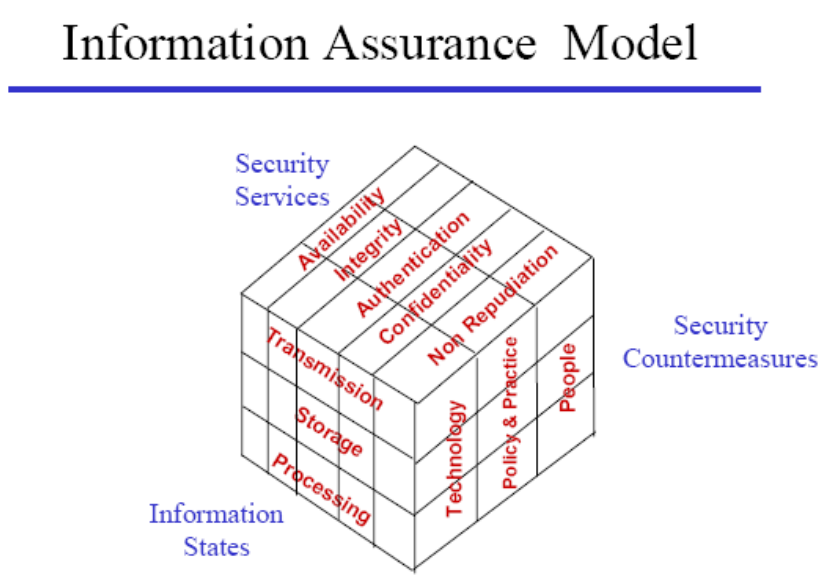


Figure 8 Information Assurance model [Maconachy, 2001, p.307]

Information Assurance is defined as:
"*Information operations (IO) that protect and defend information and information systems be ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection and reaction capabilities.*" [Maconachy, 2001, p.307]

How is information Assurance related to Information System security?

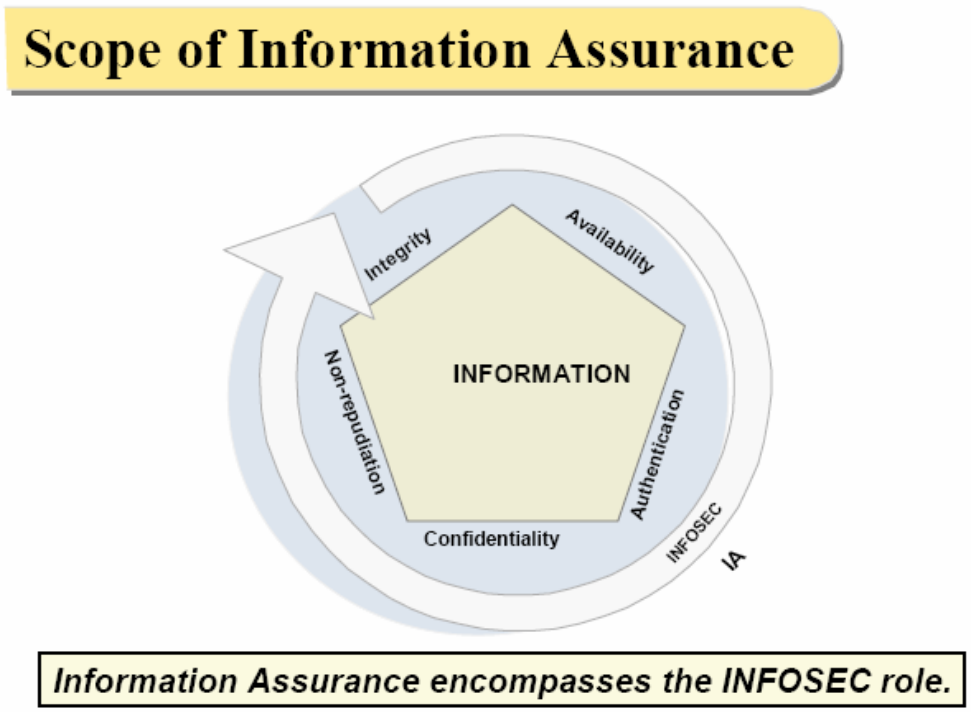


Figure 9 Relationship Between IA and INFOSEC [Maconachy, 2001, p.307]

The model has four dimensions. The one dimension is not mentioned here is “time”.

Short interpretation of the dimensions:

- Information States

Three states of information are included in the model. They nearly cover all the states of information could be now. Information could have one state or two at one time. For example, it is stored in the memory while it is transmitted to another computer.

- Security services

1) Availability: Availability is an assurance for authorized users to get access to the information when necessary no matter in what condition. For example, sometimes doctor has no access to the internet but he still needs access to patient record. Availability means to sacrifice some security function sometimes.

2) Integrity: Integrity of information confirms the accuracy of the information. That is to say, the information should be correct. Moreover, the data should be authentic enough for relying upon. That means the data shouldn’t be changed during the transporting. Integrity is an paramount indicator of information security.

3) Authentication: the person full authorized would get access to the right of process data. Otherwise the access to the data, process of data is denied.

4) Confidentiality: “Confidentiality is privacy of content” [Thomas, Loader, 2000] “In general usage, confidentiality of personal information protects the interests of the organization while privacy protects the autonomy of the individual; but, in medical usage, both terms often mean privacy.” [Sweeney, 2001, p.35]

5) Non-Repudiation: it is the proof that both the sender and the receiver could not deny how they have process, send or receive the information. Electronic signature is a famous tool for this service.

- Security Countermeasure

1) Technology: technology contains hardware, software and firewall. For example: router, workstation, server and other information foundational establishment; firewall, encryption and other security equipment; official automation system and other appropriative system; database and other normal application system.

2) Operation: User, administrator and system all could produce operation.

3) People: People are the core of security countermeasures. Why? System could be designed, calculated while people cannot. People need appropriate training and professional knowledge to protect the security of the system. People are assumed to follow the rules, policies to protect the information system. When accident beyond the management of rules happens, what is going to happen with people?

2.2 Privacy and technology

"Technology and law enforcement have a mixed relationship. Some times technology provides benefits to law enforcement, at other times it provides benefits to criminals, and most often it does some of both." [Thomas, Loader, 2000]

As said before, technology is a double-edged sword. It could provide more privacy or offer no privacy. To average people, they don't have chance to get access to high technologies today. They are not aware of what kind of private information about them is stored online either.

The minority people with high technology sophistication would protect their privacy much more. They know what kind of technology they should choose and to what extent they can put their personal information online.

2.2.1What kind of attack exists?

"In a corner of the U.S. Census Bureau, a small group of statisticians has been sweating out the agency's nightmare scenario: '**re-identification**.' That's the term for a technique that the bureau fears could allow marketers and other "intruders" to match anonymous census information with the names of the people who provided it. Such a concern is largely theoretical, so far. But if perfected, the technique could have great

appeal to marketers of everything from french fries to financial services." [Simpson, 2001]

2.2.2What kind of solution exists?

Encryption:

"Encryption can protect the privacy of personal data, including medical records. This is especially important as we begin to store more and more data with entities such as Internet service providers."[Markgren, 1984]

What is encryption?
"Encryption is the process of scrambling data using a mathematical algorithm so that content of the data is obscured." The person who is supposed to decrypt the encrypted content to plaintext (readable) should possess the "key".

The positive aspect of encryption is that it prohibits the attempt to offense data privacy, no matter what form of the information is. Of course the personal data, the medical records are included. With the dramatic growing number of patient's record transformed into electronic form, the function of encryption is rather paramount. To protect the confidentiality of email and cell phone, encryption is the best choice.

Every coin has two sides, the encryption is so. When it is used by government or authorities to encrypt information to protect the patient privacy, it contributes a lot. However, when the power of encryption is abused by criminals, it brings hardness to the sentence of criminals.

Anonymity

Being akin to encryption, anonymity is of no gainsaying value in protecting privacy. As motioned in above chapters, anonymity is the privacy of identification. Surfing online with a pseudonym is undoubtedly more secure than use your real identification.

"An anonymity web browsing service can, for example, strip all identifying information related to an individual and allow that person to 'surf' the web without

he websites she visits being able to determine who she is, or keep records of her habits tied to her real identity."[Thomas, Loader, 2000]

Also being similar to encryption, anonymity would be abused. General users of anonymity aim to protect their privacy. However, criminals use anonymity to commit crime.

Electronic Signature

Electronic signature is an electronic equivalent of a hand written signature in real life. It could only be produced by the owner of it, not anyone else. It is the representation of the identity of the owner. Electronic signature is built on the foundation of Public Key infrastructure. The arithmetic involved is Hash function.

Electronic signature offers the assurance of the information source. It is also capable to detect whether the information is altered during transferring.

Digital signature is one kind of electronic signature. It is a confusing concept. But actually it belongs to electronic signature. Electronic signature utilize digital signature to detect alteration。There are other way to achieve electronic signature such as fingerprint, retina scan，voice...Comparatively, the most mature and frequent adopted is the digital signature based on Public Key Infrastructure. As a consequence, when electronic signature mentioned, it refers to digital signature in most time.

Digital signature is very easy for transporting, very hard to be imitated, and automatically stamped with time. The assurance of the source of the information means that the signature is unique and un-deniable.

We use an example to show how the electronic signature functions:
Suppose there is a therapeutist (T) decided to cooperate with a researcher(R) to study some patient record. The therapeutist needs to make sure the identity of the researcher before he sends the information to him. Thus he decided to use the electronic signature.

1. R needs to get Private Key, Public Key and certificate from a trusted third party

which is called Certificate Authorities (CA).

Figure14.[http://www.arx.com/products/electronic-signatures-faq.php#HowESignaturesWork, 2007-5-17th]

2. R uses some software to produce a Message Digest/Hash document of the document (For example: the list of disease that he is interested in). A Message digest is unique of one document. Any slight change of the original document would lead to the change of the Message Digest.
3. The Message Digest is encrypted by R via private key to produce signed Message Digest. The encrypted Message Digest, Public Key and certificate constitute the digital signature.

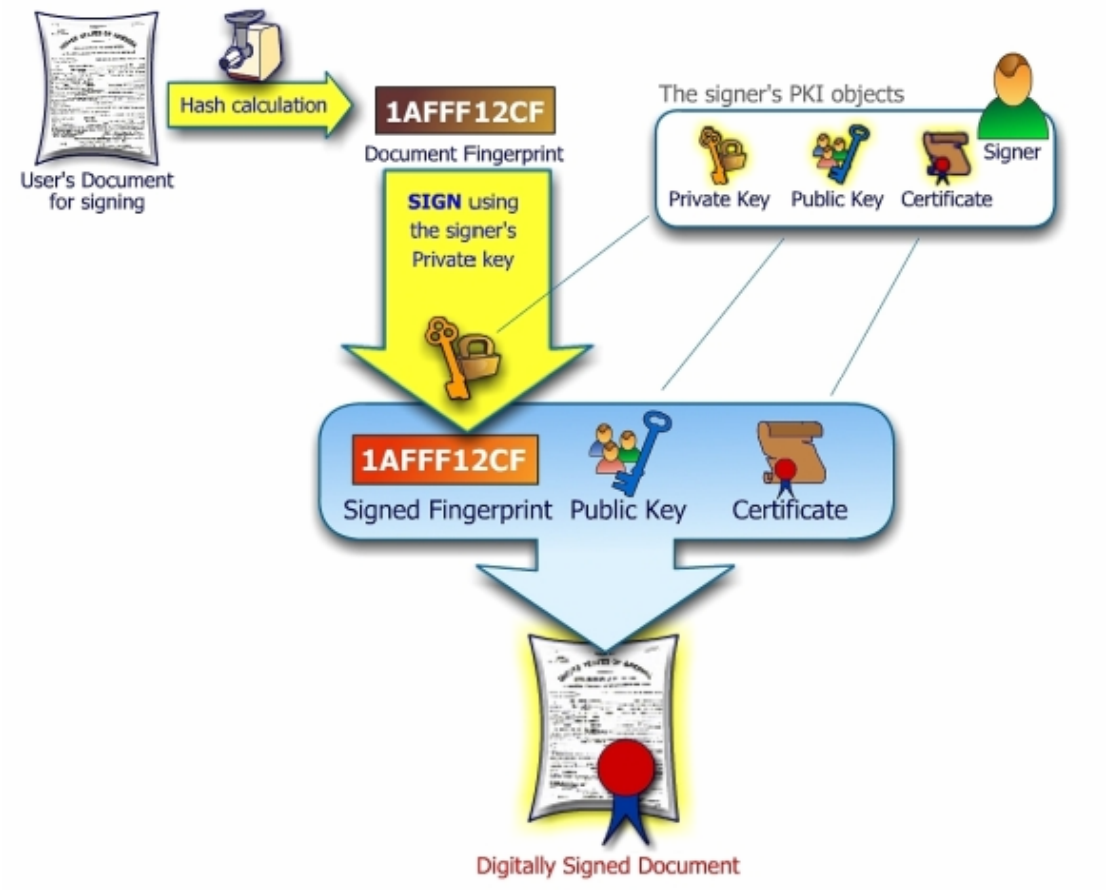


Figure 13 [http://www.arx.com/products/electronic-signatures-faq.php#HowESignaturesWork, 2007-5-17th]4. The document is signed by attachment of the digital signature.

How T verify the electronic signature? (To make sure that the list of disease is sent by the researcher?)

1. T uses the Public Key included in the digital signature to decrypt the signed Message Digest.
2. Get the Message Digest from the received document (list of interested disease) via some software.
3. Compare the Message Digest from 1 and 2. If they are the same, then the identity of R is verified and the content of the document is not changed.

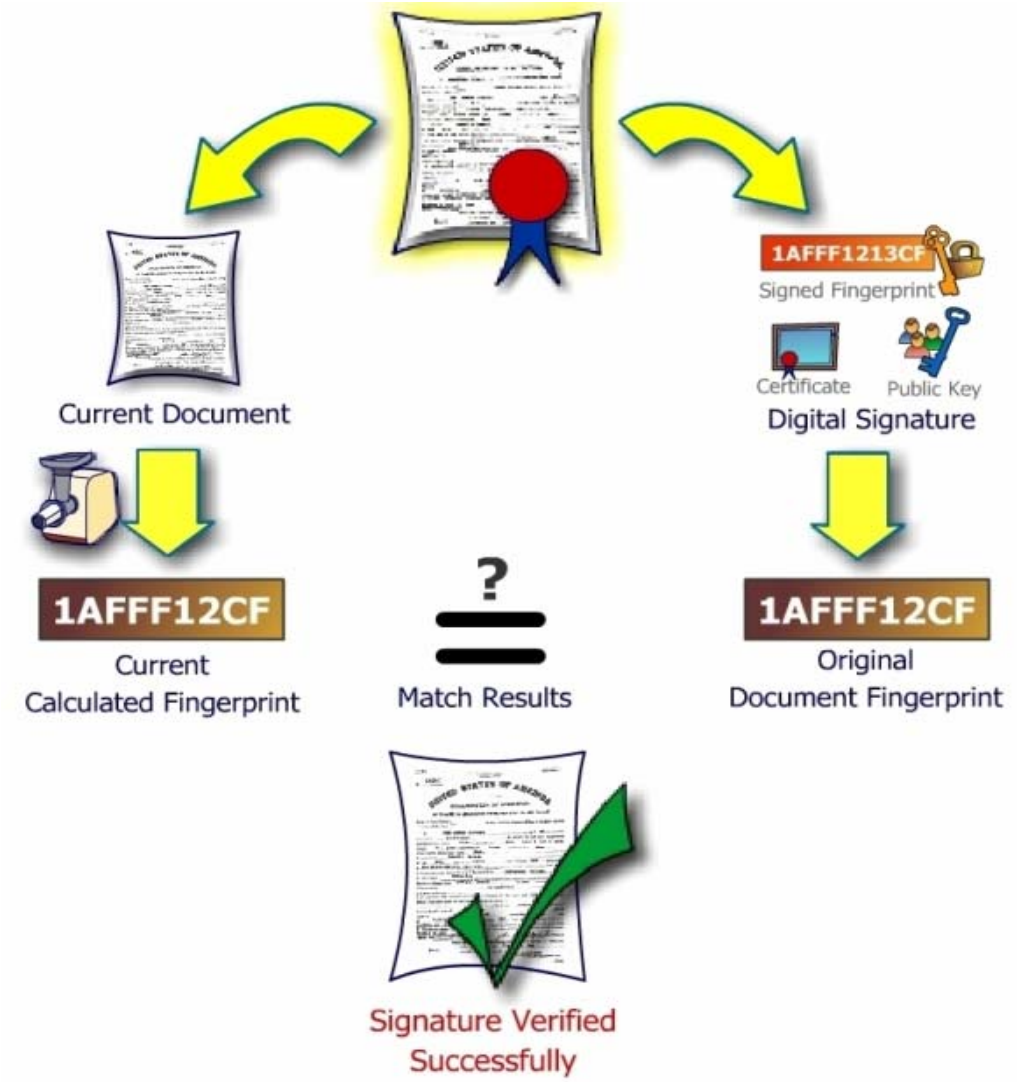


Figure12[http://www.arx.com/products/electronic-signatures-faq.php#HowESignatures Work, 2007-5-17th]

Adopting digital signature could serve as protection of information integrity during transporting, identity authentication and deny prevention (accountability).

System solution:

De-identification (DEID)

The patient record would be split into three parts, including explicit identifiers, quasi-identifiers, and non-identifying. The content of explicit identifiers is exactly as the literal meaning. The explicit identifiers contain information that are not so important such as name, social security number. That kind of information does not need privacy. Even disclosed, this kind of information will do no harm.

The quasi-identifier doesn't point straight to the explicit identifiers. But with other attributes, it could be linked to the explicit identifiers. As to the non-identifiers, it contains the important patient record that needs to be private.

If the researchers or organizations need the patient's record for study or research, the holder of the patient will give them another table instead of the original one. The released version of table doesn't contain explicit identifiers. it only contain the non-identifying and generalized quasi-identifying. The generalized quasi-identifying are much more difficult to be re-identified.

Identifying	Quasi	Quasi	Quasi	Non-identifying
Name	Social security number	Gender	Address	Brief medical record
Scofield	19781402	Female	Gothenberg	HUJGH
Sucre	19670627	Male	Stockholm	UPADK
Burrows	19450430	Female	Kalmar	EIPLSQ

The original table

Identifying	Quasi	Quasi	Quasi	Non-identifying
Unique ID	Social security number	Gender	Address	Brief medical record
aaaaaa	1978****	Female	Gothenberg	HUJGH
bbbbbb	1967****	Male	Stockholm	UPADK
cccccc	1945****	Female	Kalmar	EIPLSQ

The released table

The unique ID is a set of number produced randomly. This is for linking between the patient and the released table. Of course the linkage is only used by the holder. The third party use the data for research won't know anything about the linkage. (MALIN , 2005)

Denominalization

This model is nearly the same except for the combination of structured coding. The coding is used for relation of family. Usually six attributes consist of the original model, they are: Individual, Family, Relation, Marriage, Sibling and Multiple.

Individual is a unique number set randomly for a person. This is very similar to the unique number in DEID system. Another random number is also set for each family. All family members use this number in the attribute "family".

“Relation” represents how one family member is related to the other like sister, parents, and son. Marriage shows which marriage a child was born into. Sibling is the order of birth of children. Multiple shows which family a tuple belongs to when the individual is included in multiple families.

To which extent the patient record could be anonymous depends on which attributes are removed when information released. When the last five attributes are all removed, the record is consider to be enough anonymous. (MALIN, 2005)

Trusted Third Parties and Semi trusted Third Parties

Encryption and Decryption are used in TRUST system and SEMITRUST system.

There are two protocols-the subject discovery protocol and transferred protocol. Only the subject protocol will be described briefly here.

The protocol is started with researchers getting in touch with the physicians who attend the patient has the disease that the researchers are interested in. A list A{Name, Social Security Number, Additional Demographic Features§, Disease}is sent to the Trusted Third Party by the physician. The Trusted Third party encrypts the social security number by encryption function f. then the social security number becomes f (Social Security Number). Secondly, the Trusted Third Party will send the table A'{f (Social Security Number), Disease} to the researchers.

There may be some records are interesting to the researchers. They would send a wish list for further study to the Trusted Third Party. The list includes the encrypted Social Security Number. The Trusted Third Party decrypts the list to get the social security number and forward the name and social security number to the physician.

The SEMITRUST system employs the semi trusted party for transferring data. The semi trusted third party doesn't have access to plaintext (readable). They are only trusted to deal with the encrypted data.

Before the semi trusted third party receive the data from the hospital or the other data holders, the identity of the patient is already encrypted by the data holder. The researchers receive the data that are double encrypted both by the data holder and the semi trusted third party. If the researchers are interested in some of the data, they can send the list of double encrypted identities to the emigrated party. Then the semi trusted third party will decrypted the list into single encrypted identities and send it back to the data holder for further information. (MALIN, 2005)

2.3Law and ethical view of data privacy

"Technology can go a long way toward protecting the privacy of individuals, but we also need a legal framework to ensure that technology isn't outlawed (Bernstein: http://www.eff.org/bernstein/.) We can't protect privacy through case law, and self-regulation hasn't worked."

Deborah Pierce

"Yes, safeguards can be built into any system, such as the checks and balances in a good accounting system. But what keeps them in place is not the technology, but people's commitment to keeping them.

We cannot expect technology alone to solve ethical dilemmas. Technology is a tool made by people to meet people's needs. Like all tools, it can be used in ways undreamed of by the inventor. Like all tools, it will change the user in unexpected and profound ways." [Weiser, 1995]

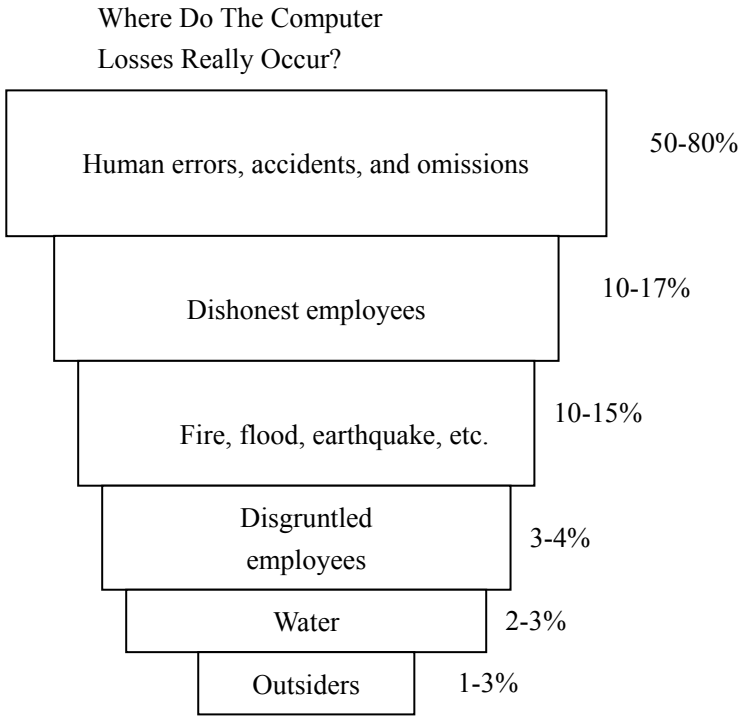


Figure 5 Computer Losses (Forcht, 1994)

Beyond half of the technical profession believe that when the current and former employee of the hospital try to put the system in danger, security technique, policy and training can offer little help in preventing them to produce security hole。Judging this situation, the law/acts should be a better way to protect the patient's privacy. This part of the thesis will discuss the law/acts from large scale to small scale.

The Law included in this part is presented from international to local.
"The Universal Declaration of Human Rights states in its article 12 that:

No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, or to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks. "[Wikipedia]

What is concerned in this thesis is protecting patient privacy in e-health care. This is a rather narrow area of data privacy, but the issue rose in this condition still needs to obey the law and ethic of data privacy.

As a member of European Union, Sweden is one of the signatories of European

Convention on Human Rights and the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (1981).

Except for this, Sweden also has its own law to deal with data privacy concerned issue.

The earliest, foundational law of Swedish data privacy is the Data Protection Act (Datalagen) (1973).

"On the 24th of October 1998 the Personal Data Act (1998:204) came into force and replaced the out-dated Swedish Data Act from 1973. The Personal Data Act is based on Directive 95/46/EC which aims to prevent the violation of personal integrity in the processing of personal data. However the processing of personal data that commenced before the 24th of October 1998 is still regulated by the Data Act, 1973. This transition period will apply until the 30th of September 2001."[http://www.datainspektionen.se/in_english/personal_data.shtml]

There are a set of laws/act related to Data privacy in medical area below:

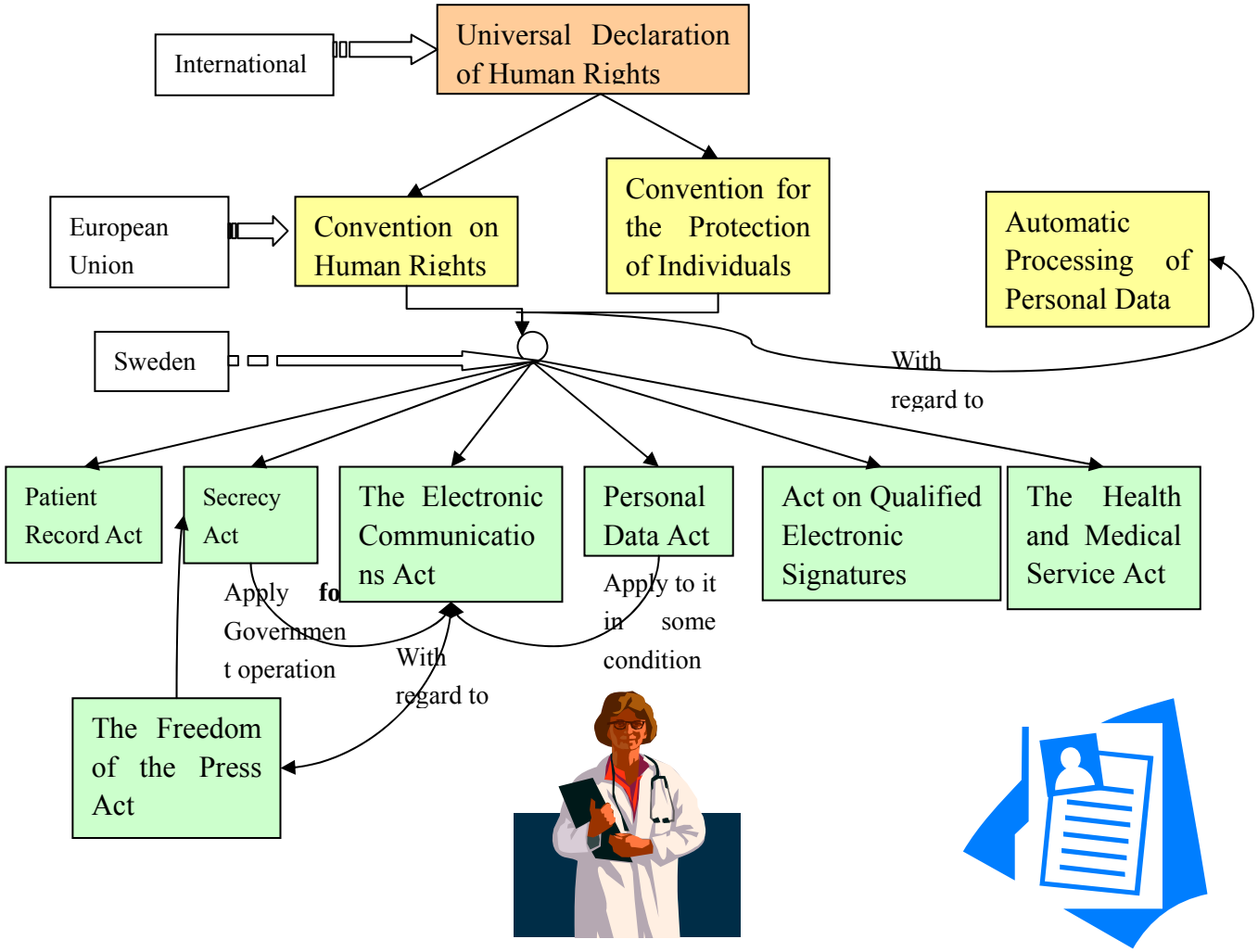


Figure 6 the relation between laws/acts

1. Secrecy Act:

"The Secrecy Act, which entered into force on 1 January 1981, contains provisions on what is to be kept secret in state and municipal activities."[The Ministry of Justice, "Public Access to Information and Secrecy with Swedish Authorities", p.4]

In the Act, the concept of secrecy is concluded. Secrecy means "a prohibition on disclosing information whether orally or by making an official document available or in any other way"[The Ministry of Justice, "Public Access to Information and Secrecy with Swedish Authorities", p.4]. Secrecy Act also set a limitation for public to access documents that should be kept secret.

Personnel protection is described in Chapter 7 of Secrecy Act. Chapter 7 protects the health care, social welfare and other personal circumstances of the individual. In

chapter 14, there is rules focus on criterion and reservation when individual gets access to information.

If damage is assumed to be caused by the disclosure of personal information, the Secrecy Act will be applied.

For authority getting access to information, the Secrecy Act does not prevent this action in most cases, especially when the interest of providing the information is more than preserve the information. However, this condition is not applied in healthcare, medical and social welfare areas.

2. The Freedom of Press Act

The Freedom of Press Act sounds to be in the opposite position of the Secrecy Act. Actually it also mentioned that the Freedom of Press should be within the scope that the nation, personal right are not harmed. This is the prerequisite. It is said in Chapter2, Article 2, "The right of access to official documents may be restricted only if restriction is necessary having regard to 1. The security of the..." The protection of the personal or economic circumstances of private subjects is included in this set of restrictions.

3. Patient Record Act

Although the Patient Record Act came into force as early as 1985, it offers the provision of personal medical record in paper form or other medium form. Anything which contains medical information belongs to the government of this Act. People of special certifications, therapist, psychologist or psychotherapist are appointed to be responsible for patient records.

The Patient Record Act regulates the content of the patient record. It says a standard patient record should include identify, anamnesis, diagnosis, the treatment and requirements of care. The person who is appointed to be liable for the record should sign after every notation is made if the notation is permitted.

It should be made clear that the Patient Act is managing the interior secrecy of the patient data. The exterior secrecy of patient record is regulated by the Secrecy Act

[1981] In Patient Record Act, unauthorized access to patient record is forbidden. Only the person works as the clinician or therapist will get access to the patient record when necessary.

4. Personal Data Act

Personal Data Act [SFS 1998:204] replaces the old Data Act [1973] because many chapter of Data Act [1973] is outdated. For example, the Data Act only set restriction on personal data when it is automatically processed while the Personal Data Act take the manual processing of personal data into consideration in some cases. This act came into force with the objective of protecting the personal data from encroachment. It mainly concerns about the processing of personal data (collection, registration, storage, processing, disclosure by transfer and compilations or joint processing).

The Personal Data Act is the foundation for protection of personal data. Many other acts put more detail of privacy protection. Thus when the freedom of the press and freedom of expression limit the access to the information the Personal Data Act does not apply.

The medical records, as one of the sensitive personal data, are under the protection of Personal Data Act. "It is prohibited to process personal data that discloses race or ethic origin, political opinions, religion or philosophical convictions and membership of trade unions. It is also prohibited to process personal data related to health or sexual life" [Sweden Ministry of Justice, "Personal Data Protection-Information on the Personal Data Act"]

As well as other personal data, approval of registered person should be got for permission of processing patient personal data. When the data is used for preventive medical diagnosis, care or treatment, or the administration of health and hospital care, the consent is not necessarily needed. In a word, if the information is needed for the significant interest of public, personal data could be processed without approval.

5. The Health and Medical Service Act (1982:763)

In the health and Medical Service Act, the privacy of patient is mentioned in Chapter2, Section2 a: "Health and medical services shall be conducted so as meet the

requirements for good care. In particular that they must...3.be founded on respect for the self-determination and privacy of the patient," It is also mentioned in Chapter2, Section 2b, when the information disobey Chapter 7, Section 3 or 6 of the Secrecy Act [1998:100] or the Section 8, 9 of the Health and Medical Services Act, the patient information could be neither given to himself/herself or to her/his relative.

6. The Electronic Communications Act (2003:389)

The aim of Electronic Communications Act is "ensuring that private individuals, legal entities and public authorities shall have access to secure and efficient electronic communications and the greatest possible benefit regarding the range of electronic communications services and their price and quality"

This act is involved in the process and transmits of information. As a consequence, it also involved in the data privacy and security.

Chapter 6, section 3 gives the provision that any party should take proper approaches towards data security when it offers the public electronic communications service. Chapter 6, Section 4 says that if there exist certain risk, the subscriber should be informed.

"As regards the processing of personal data in connection with the provision of Electronic communications networks and electronic communications services and in connection with subscriber directory services, the Personal Data Act (1998:204) applies, unless otherwise prescribed by this Act."[The electronic Communications Act]

Chapter3. System security evaluation

According to the needs of computer security, the safeguard of information system is a everlasting cycle to insure that the system to be more and more secure. This cycle goes through the whole life period of information system. The measurements of safeguards contain risk prevention measurement, security testing and evaluation, security response.

Among the three measurements, the testing and evaluation of security function as the

tool to check the security status of information system. To see if the cooperation of components could function best and if the goal of system security is achieved. And then it offers suggestions about improvement of security.

The evaluation of security is the essential method and measurements of prove the security of information system. Evaluate the security status of system once upon a time is important. Predominate the current security status adds strength to modify the flaw and shortage of the system. The more attention is paid to the evaluation of the security of the system, the more safeguard of the information security is.

In this chapter, an information security evaluation model of information system will be set up. The information security evaluation in other countries will also be mentioned.

3.1 Information system security evaluation

In the investigation process of information system security evaluation, the related content is generalized, including evaluation criterion, evaluation process pattern, evaluation technique method.

1) The evaluation criterion is the related standard that should be obeyed in the process of evaluation, including main content of evaluation, main conclusion of evaluation, the technique adopted and the patterns of evaluation process. This is the critical reference of evaluation. Only when the evaluation is done under standard, the result is comparable. In Sweden, the SIS, Swedish Standards Institute offers all Swedish, ISO and IEC standards.

2) The evaluation process pattern consists of evaluation actors and the related responsibility, evaluation process, evaluation conclusion format. The information system security evaluation should be under the guidance of evaluation patterns.

3) Risk analysis technique, safety testing technique and security evaluation technique composes evaluation technique method. Evaluation technique method is the practical tools in real life.

3.1.1 Evaluation standard

In the Information system evaluation, the first, most necessary is the evaluation criterion. It is the direct reference of evaluation. Checking the information security according to the criterion and get the conclusion is the right way. The criterion should be authority, justice, performable, practice, and effective. Different information security evaluation should be processed in accordance with one standard. The result of the evaluation could be comparable then. Moreover, the evaluation criterion should be put in different hierarchy; the inferior level of standard should obey the upper level of standard.

The evaluation objectives include router, workstation, server and other information foundational establishment; firewall, encryption and other security equipment; official automation system and other appropriative system; database and other normal application system. Facing evaluation of these information systems, not only one but multiple criterion should be set aiming at a specific kind of system.

Moreover, the information system security evaluation should cover the whole life period of information system, including design, development, install and application. In every stage of the life period, evaluation should be applied. The goal of security could be achieved. The security evaluation criterion would also have this characteristic. Criterion should cover the evaluation of all stages of the life period of the information system.

Sweden's organization evaluates the IT security is CSEC. The criterion it adopts is the "…the standard ISO/IEC IS 15408, also know as Common Criteria…" (http://www.fmv.se/WmTemplates/Page.aspx?id=824, 2007-5-23rd)

The Common Criteria (CC) defines three aspect of evaluation:

- "IT security requirements for products ('protection profile' – the user's requirements)
- IT security requirements and features for a specific product ('security target' – the vendor's commitments)
- Rules and method for independent evaluation of IT products with respect to the document above ('Common Evaluation Methodology', CEM – specifying the

evaluator's work)"(CSEC – The Swedish Certification Body for IT Security)

3.1.2 Evaluation pattern

A formal evaluation strategy and process is the first and critical qualification of information system security status evaluation.

For example, America has patterns as NIAP (National Information Assurance Partnership) and TTAP (Trusted Technology Assessment Program). These two patterns allow authorized business laboratory to evaluate the information security under a universal standard. The result of the evaluation will be written to the evaluation product list (EPL).

England use ITSEC to evaluate IT product and system. The evaluation is done by the registered commercial organization.

In Sweden, the CSEC is appointed to be the Swedish Certification Body for IT Security. "In accordance with the decision of the Swedish parliament in May 2002, CSEC is responsible for the establishment, operation and administration of system for evaluating and certifying IT security products and systems" (http://www.fmv.se/WmTemplates/Page.aspx?id=824, 2007-5-24th)

3.1.3 The evaluation technique

Risk analysis technique, safety testing technique and security evaluation technique composes evaluation technique method. The base of information security evaluation is risk analysis and safety test conclusion.

Risk is the potential or possible risk factor. The three steps of risk analysis are 1: confirm risk; 2: confirm the threat of risk; 3: balance the lost caused by risk and the profit gain by risk prevention measurement. Risk analysis confirms safety fragility. It contributes to taking the profit gained from cost of safety into consideration.

Risk analysis is the first step of information system security evaluation. Take control of the information system construction, the risk faced, current fragility, possible loss

through the risk analysis of information system. The conclusion of risk analysis would be used as the input of safety evaluation.

Safety testing technique not only contains explicit defined index such as firewall defence testing, decryption prevention testing but also contains security function robust testing, IT security product characteristic testing. The result of safety testing is also the input of information security evaluation.

3.2 How the IT security is evaluated in Sweden

The "Security Target" established by the sponsor is referenced when evaluation entails the evaluation of a product. Protected assets, product used environment, present threats and IT security function ensures the security of the product are described in detail in the "Security Target". Adding confirmation of the product to resist the existing threats is the goal of evaluation. (FMV, "Evaluation and Certification")

What is certification? It is the result of evaluation mentioned above. "This determination entails seeing to it that the evaluation task is carried out with the necessary precision and according to approved methodology, as well as the result of the evaluation tasks showing that the product satisfies the prescribed requirements as well as a defined level of assurance as stated in the Security Target. The level of assurance states the degree of confidence n the security functions in a product or a system."(FMV, "Evaluation and Certification")

Universal standard – Common Criteria (CC) is obeyed in the process of evaluation. A common methodology for Information Technology Security Evaluation is included in the criteria. How the requirements should be evaluated is not only included in CC but also included in the Evaluation and Certification Scheme.

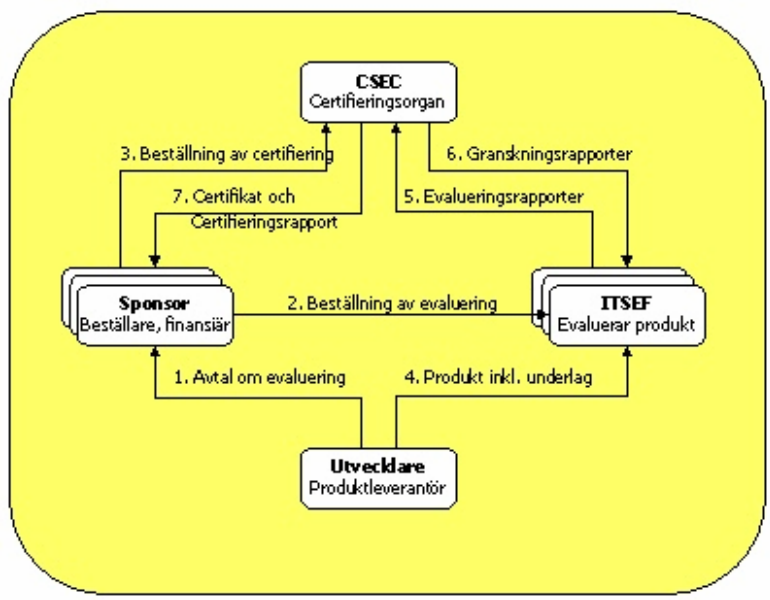


Figure 7 the process of evaluating and certifying

Explaining of the figure:

- CSEC is mentioned in the above 3.1.2, it is the Swedish Certification Body for IT Security. "CSEC is responsible for the establishment, operation and administration of system for evaluating and certifying IT security products and systems" (FMV, "Evaluation and Certification")
- ITSEF is short for IT security Evaluation Facility.
- The Sponsor is the one who ask for a evaluation and the one who pays for the cost of evaluation.
- Utvecklare (Swedish) – The company who develop the products

The following are the explanation of the process written in Swedish:

1. Evaluation agreement

There is a difference between the evaluation of the product at assurance level EAL 2 or higher and those are at level EAL 1. The formal kind of products needs the Sponsor, the developer and the examiner while the later one only needs the Sponsor and the examiner. It is because the technical product document should be used in the formal circumstance.

2. Ordering of evaluation

The Sponsor is the one who order the evaluation with the ITSEF. ITSEF is the party

that would be the examiner of the product.

3. Ordering of certification

The Sponsor sends all the files needed for applying the evaluation to the CSEC. The CSEC then gives a tender to the Sponsor. The Sponsor needs to order a certification according to the tender.

4. Product including basic data

In the formal kind of evaluation – products at the assurance level 2 or higher, the developer should offer the basic data of the product at the beginning of the evaluation.

5. Evaluation reports

The Evaluation is done under the guidance of the Evaluation Methodology. Different aspects of the product are examined and the result of this examination are written into a report and sent to the CSEC.

6. Examination reports

The CSEC check the evaluation report from ITSEF and send it back to ITSEF for final decision.

7. Certificate and certification reports" (FMV, "Evaluation and Certification")

The final decision of the status of the product security is decided by the ITSEF. And the final report is sent back to CSEC for a formal certification.

Chapter4. Case

This chapter mainly talks about the case. Where the case takes place? What is the aim of the case? How the case is designed? Why it is designed in this way? These questions could all get an answer in this chapter.

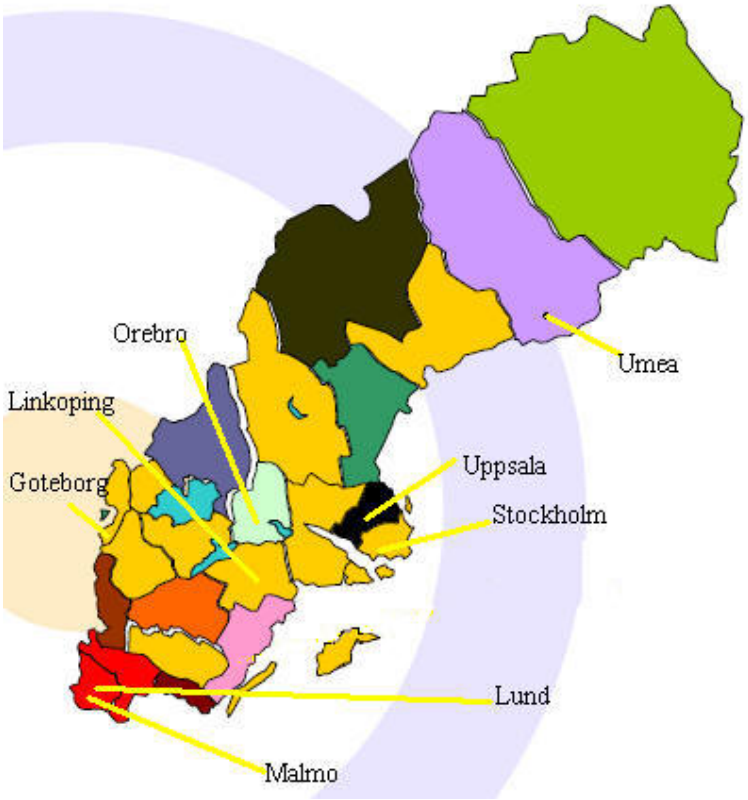
4.1Workplace

The aim of the thesis is to give out suggestions about how to improve the patient data privacy through study the security situation of the e-health care in Sweden. Judged from the background of Swedish health care, it is decided that the case study would be

take place at the regional hospitals. Going too deep into the technical is not the aim of this report.

The place for interview depends on which hospitals would agree to make an interview with me. The observation would be done by interview, telephone and emails. Of course the ideal way to get the particular data is by face to face interview.

The initial plan for investigation is to make interview, phone call or email with 3-6 hospitals in Sweden.



As the map shows, there are eight regional hospitals in Sweden.

To make interview with all of them is too huge work. The work would also be too generalized.

Given that not every hospital would agree to make a face to face interview in English with a foreign student, I also would offer the option of phone call and email.

Figure 10 work places

4.2 design of questionnaire

As we mentioned above, the case will be interview with the regional hospitals about the approaches they use towards data privacy/information security. It is presented in the form of questionnaire. 7quesions are designed aiming at see into the way regional

hospital security staff use when dealing with the personal data problem.

The first question is "Do you use technique for data privacy/security?" As far as I know, the adoption of EPR in secondary healthcare (hospitals) is 30-35%. Among the nine regional hospitals, there are some of them seldom use electronic prescription, and some of them only put some strength on EPR. It is necessary to know that when EPR and electronic prescription are not used very often in the system whether the system would not pay attention to the technique of maintain information security.

If the answer of the first question is "Yes", then comes to the second question. It is asking what kind of technique is used in the information security. The people who said "No" to question one can skip this question to question 3. Question 2 aims to get to know what kind of information security protection technique is often used in different regional hospital.

Those who finished question one answered "No" and finished question 2 would go to question 3. The third question help to give profile of those hospitals that are not using too much ICT and information security in their daily work. It is supposed that they don't use the technique for data privacy/information security because that they don't utilize too much ICT in healthcare. They should tell that what approaches they are using. At the same time, it is also important to know what other approaches those hospitals that have used the techniques.

If question 1 and 2 aim to get to understand what kind of techniques are used in different hospitals, the purpose of question 3, 4 and 5 are to understand what kind of laws/acts are paid attention to in the hospital. More attention should be paid to this part because it is discussed in 2.3 that employees and interior threats are more dangerous than those exterior threats.

Question 6 tries to show what rules the hospital follows when processing patient's personal data. For example, if a researcher wants to get some data of a special disease, what principle they should obey to negotiate with the hospitals.

Question7 is an end question. After all the acts, laws, techniques, what threats still

exist? What kind of problems the hospitals are facing?

4.3 How the case is done

Sweden's regional hospitals

Karolinska University Hospital, Stockholm
Karolinska Universitetssjukhuset
www.karolinska.se

Sahlgrenska University Hospital, Gothenburg
Sahlgrenska Universitetssjukhuset
www.sahlgrenska.se

Uppsala University Hospital
Akademiska sjukhuset i Uppsala
www.akademiska.se

Lund University Hospital
Universitetssjukhuset i Lund
www.usil.se

Malmö University Hospital
Universitetssjukhuset MAS
www.umas.se

Linköping University Hospital
Universitetssjukhuset i Linköping
www.lio.se/us

Norrlands University Hospital, Umeå
Norrlands Universitetssjukhus
www.vll.se/umea

Örebro University Hospital
Universitetssjukhuset i Örebro
www.orebroll.se/uso

According to Figure 15, the author visited every website of regional hospitals. Except for two hospitals have no English version or ways of contact, the email of all the other hospitals are found out. An email was sent to each of them. After one week, there was no reply at all.

Then all of those websites are visited once again and all telephone numbers for contact are found and listed.

From 29th of April, phone calls are made with each hospital for the ways of contact of the information security man. For not understanding enough Swedish, the phone calls are made in English.

Figure15 websites of regional hospitals (Fact sheet, "Swedish health care", 2007)

For being a foreign student who needs help from the information security man in the hospital, the author has to explain a lot about herself, about the thesis and her honesty for applying the result anonymously.

For one thing, the job of information security man has its particularity, the operator sometimes didn't want to give out his personal telephone number directly but help the author to be connected to the security man. Once the telephone is disconnected, the author has to start from the operator once again. When it is another operator answers the phone, the author should explain herself once again.

For the other thing, the jobs of the information security man are very busy. They

always have several projects on hand at the same time. Sometimes they would travel on business or on vacation for about more than a week.

The above two reason could tell why it seems very simple to get in touch with only 8 information security men but actually took nearly a month before getting the answer to the questionnaire.

Because this took really too long a time, there is no time to ask for more detailed answers before the deadline of the thesis. There is some misunderstanding of the questions in the questionnaire for the security man and that would leads to the hardness of analysis of the results. Everyone knows if a face to face interview is taken then the misunderstood would be decreased a lot but that would take even more time for making an appointment with the information security men.

4.4 result of the questionnaire

After contacting with 9 regional hospitals, I got four answers to the questionnaire. The questionnaire is anonymous so I mark them as Hospital A, B, C and D.
Please see to the end of the thesis for questions in the questionnaire:

Hospital / Question	A	B	C	D
1	Yes	Yes	Yes	Yes
2	Almost everything of the listed techniques…	B1 B2 B4 B5 B6	B1 B2 B6 C1	A2 B1 B2 B3 B4 B5 B6 B7 C1
3	Law/Act X Rules X Else Yes…	Law/Act X Rules X Else N/A	Law/Act X Rules X Else N/A	Law/Act X Rules X Else: Ethics, Informationbooks from datainspektionen(The Data Inspection Board).
4	There are MANY important rules… User rules, technical	You must be part of the team treating the patient to	The rules in the hospital are based on the laws and regulations. The punishment	Personuppgiftslagen(personal data act), Sekretesslagen, Patientjournallagen, Vårdregisterlagen,

	rules, security issues a s o. Malicious code, role based access a s o.	access the data	depends on to what grade the abuser abuse the data. The authorized workers should sign a document, state what is allowed and what is not allowed.	Tryckfrihetsförordningen.(reedom of the press act)
5	Patientdatalagen (patient data act), to mention one.	Swedish law on privacy (Sekretesslagen)	Secrecy Act, Personal data act,	Tryckfrihetsförordningen, Hälso- o sjukvårdslagen(medical care act), Arkivlagen(archive act), Lagen om hälsodataregister(health computer file act).
6	N/A	Pseudonymisation of data	Personal data act,	Vårdregisterlagen. We also follow the descitions by Etikprövningsnämnden(Ethic trial board).
7	Many… Economy, technical, user based, competence…	Methods to check the log files on a regular basis	Electronic Journal, what does people do with patient data is reported Encryption, according to the Personal data act.	It is an ongoing work to find a good balance between patient privacy

Table 3 answer to the questionnaire

Chapter5 Discussion

What does the result of the questionnaire mean? This chapter gives an analysis of the results applying the theory and model described in former chapters. After the analysis, a discussion about how to apply the results in future study will be carried out.

5.1Case Analysis

Q1：According to the answer of the fist question we see that all of those hospitals use technique to protect the information security. It shows that hospitals really care about patient data privacy and shows emphasis on it to some extend.

Q2：Let us have a look at the frequency of utilization of the techniques:

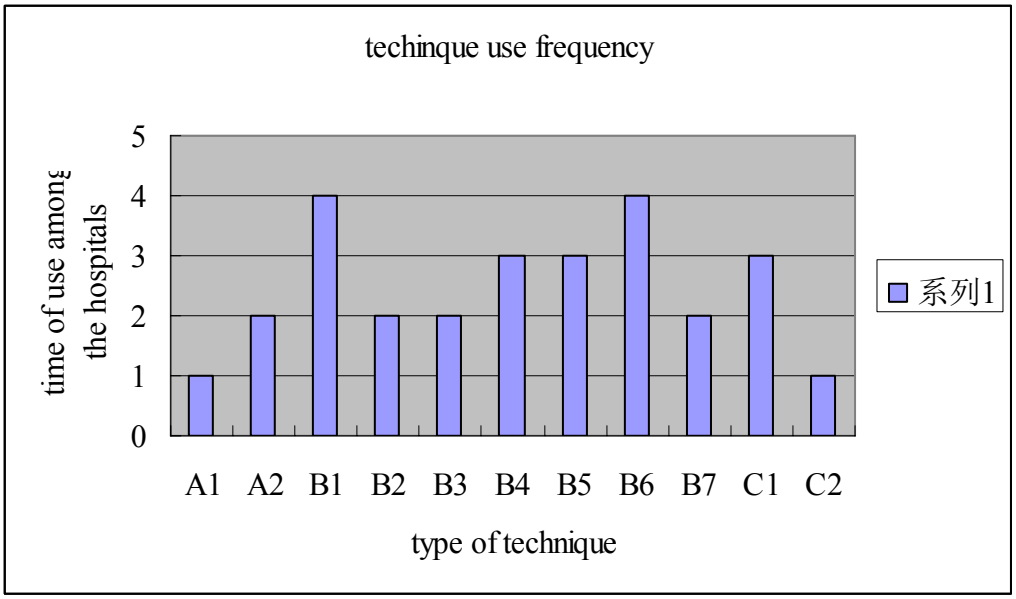


Figure 11 technique use frequency

For the types of technique please refer to **Appendix1 Summary of technologies applicable to information system security management. [12]**

Judged from figure, the most frequently used type of technique is B1 and B6. They are

B1.Authentication	Determine who is connecting	Accounts/passwords, Kerberos, tokens (e.g., Secur-ID), public-key systems, biometric systems
B6.Firewalls and network service management	Define system perimeter and control means of access	Many Vendors

Authentication is one of the security services in the Information Security Model in 2.1.3

The second frequently used techniques are B4, B5, C1, they are:

B4.Digital signatures	Validate notes and orders	Evolving standards
B5.Encryption	Prevent eavesdropping	PGP, Kerberos, DES, public-key systems, secure sockets
C1.Software management	Guard against viruses, Trojan horses, etc.	Tripwire and controls over loading of uncertified software

Encryption, as described in 2.2.2, is the most commonly used tools for the safety of

data. Although it adds to the difficulty of detecting cyber criminals, it is still necessary in information security.

Digital signature is a typical tool to serve as the non-repudiation in the security services in the Information Security Model in 2.1.3.

The hospital A's answer to Q2 is "Almost everything of the listed techniques…" Thus all of those techniques are at least used by one of those hospitals. Thus we could get the idea that nearly no hospital use A1 and C2 except hospital A.

A1.Alerts and reminders	Reinforce user ethics	Vendor-specific
C2.System vulnerability analysis tools	Detect unintended system vulnerabilities	SATAN, crack, National Computer Security Association

This doesn't mean that these two techniques are not useful. Actually, alerts and reminders for reinforce user ethics is very important. As mentioned in 2.3, both the description and figure 5 give the warning that interior abuse of patient's data is more dangerous than outsiders. Ethic and law should be paid more attention. A1 is represent the technique for enhance ethics of user thus it is very paramount. C2 is used to detect unintended system vulnerabilities. This is one of the steps of information security evaluation. Information security evaluation should be done once in a period to prove the ongoing process to improve the system.

The other hospitals doesn't use these two techniques should consider adopting technology in these two categories.

A2, B2, B3, B7 are used by half of the hospitals.

A2.Audit trails	Document access/give alerts	Custom research systems and some vendors
B2.Authorization	Define who can access what information	OS file and database vendor access controls, DCE access control lists
B3.Integrity management	Ensure information content is as intended	Cryptographic checksums
B7.Rights management tools	Control information distribution and access	IBM Crypto-lopes

Q3.

All of the hospitals follow both the law/act and the rules in the hospital. We then could know what the laws/acts are in following questions. Hospital D tells that they also use ethics, and they follow the information-books from the Data Inspection Board.

Q4.

The most import rules in the hospital about data privacy are listed.
In hospital A, it is said that "There are MANY important rules… User rules, technical rules, security issues and s o. malicious code, role based access and s o."

In hospital B, it is said, "You must be part of the team treating the patient to access the data"

In hospital C, it is said, "Rules based on the laws, Regulation,
Depends on the grade of what the abuser
Sign a document, state what is allowed and what is not allowed."

In hospital D, it seemed that the security man take the most important rules as laws and act. Then no rules of the hospital are mentioned here.

Q5.

5	Patientdatalagen (patient data act), to mention one.	Swedish law on privacy (Sekretesslagen)	Secrecy Act, Personal data act,	Tryckfrihetsförordningen, Hälso- o sjukvårdslagen(medical care act), Arkivlagen(archive act), Lagen om hälsodataregister(health computer file act).

The laws listed here include Patient Data Act, Secrecy Act, Personal Data Act, Freedom of the Press Act, Medical Care Act, Archive Act(or Document Act), Health computer file act. Those are not included and mentioned in the thesis are Medical care Act, Archive Act and Health computer File Act.

Q6.

6	N/A	Pseudonymisation of data	Personal data act,	Vårdregisterlagen. We also follow the descitions by Etikprövningsnämnden(Ethic trial board).

For patient data processing, hospital B uses pseudonymisation. It is in the category of anonymity. Hospital C follows Personal Data Act when processing the data. Hospital D follows the Care Register Act and the decision by Ethic trial board.

Q7.

7	Many… Economy, technical, user based, competence…	Methods to check the log files on a regular basis	Electronic Journal, what does people do with patient data is reported Encryption, according to the Personal data act.	It is an ongoing work to find a good balance between patient privacy

It seemed that people don't quite get what I mean when I ask "what problem exists in information System security" or it is not convenient for them to answer. In other words, if the criminal knows the problem exist they may take advantage of the flaw and shortage of the system and try to attack. Thus I didn't get any analysis from this question.

5.2 suggestions for future study

Neither the design of this case nor the study of the case is thorough. There are mainly two reasons: On one hand, as it is said before, the questionnaire is only sent to 8 regional hospitals in Sweden for the time and human resource limitation. After a long period of telephone contact, only 4 information security men from different hospitals sent back the answers to the questionnaire. On the other hand, for the lack of deep knowledge and experience in the field, several aspects of the case are lack of consideration.

The study of this thesis could both be a research and a process of learning for the author. For future study, if another author would like to study the same area as this thesis, the result of this thesis could be applied as a foundation of study. The information security model in this thesis could be used in a general level no matter which country the future author will study. The design of the questionnaire could be a

basic cue for him, too. On the base of the questionnaire in this case, the future author could improve it with his knowledge. If the author does not study alone but study in a group, with more time and human resource, the questionnaire could be sent to more organization like hospitals (65), health center (1000) and regional hospitals. A more thorough result could be getting with more questionnaires. If the future author decides to concentrate on one hospital, the questionnaire could also be applied. But it should be applied in a more detailed way. More questions, deeper study and larger scale of structure could be included.

Chapter6. Conclusion

The answer of the questionnaire tells a lot of information about data privacy approaches in regional hospitals. From the first question we know that all the hospitals pay attention to the technique of information system security. From the second question it is considered that A1.Alerts and reminders and C2.System vulnerability analysis tools should be attract more attention. Every hospital has its strength and weakness. It is hard to judge the strength and weakness here because there are only four answers to the questionnaire. Too little material and opinion would lead to conclusion that is not objective. But one thing should be confirmed here is that they should learn from each other to build a more secure information system. As a consequence, the data privacy will be fully protected.

After survey the approaches towards data privacy in different hospitals through questionnaire by interview and email, on one hand, more knowledge of data privacy and information security are gained. It is obvious that several factors in the Information Assurance Model in 2.1.3 are mentioned and realized in reality such as authentication, integrity, non-repudiation, technology and processing. Technology and laws/acts mentioned in above chapters is also mentioned in the questionnaire.

It proved that the formal study are valuable in reality and give basic knowledge to the beginners to some extend. On the other hand, some technology and laws/acts mentioned in the questionnaire are not included in the thesis. It shows the limitation of the thesis. First I cannot get access to some of the laws/acts because they are not

translated into English. Secondly, I am lack of knowledge about information security. The process of writing this thesis is actually a process for me to learn more about this field. I find places that I am weak in and gain more knowledge than before.

For time limit, the questionnaire is designed before the writing of 3.1 Information system security evaluations. The answers to the questionnaire are also got before this part. However, after writing this part about information system security evaluation, I found that several other questions should be added to the questionnaire to know more about system evaluation. It is too late to send the questionnaire to hospitals to ask them to do it again but the modified version of questionnaire may give some help to the students who write thesis in this field in the future. The modified questionnaire is also at the end of the thesis. The former questions of the questionnaire are still needed. The reason could be judged from 4.2 design of questionnaire.

Why the first question should be kept? (1)It is said in chapter 1.2.2: As far as I know, "The French IT consultancy company Steria is one of the major players in security solutions." [Tarre, 2003, p.10] But in the following six regions, only Stockholm/Kista adopts the Steria. The six regions are 1, Linköping/Norrköping, 2.Norrbotten/Västerbotten, 3.Skåne, 4.Gothenburg, 5.Blekinge, 6.Stockholm/Kista. I don't know what kind of approach the other regional hospital use towards data privacy and if they are enough for protecting the patients' privacy. (2)It is also discussed in chapter 4.2: the adoption of EPR in secondary healthcare (hospitals) is 30-35%. Among the nine regional hospitals, there are some of them seldom use electronic prescription, and some of them only put some strength on EPR. It is necessary to know that when EPR and electronic prescription are not used very often in the system whether the system would not pay attention to the technique of maintain information security. Every part of the thesis set foundation for the following part. Each question of the questionnaire has its root. But on this basis, I think the evaluation questions should be added to the original questionnaire.

References:

1. Szolovits, Peter, "Patient Data Privacy in Electronic Records.", 07 March 2002, <http://groups.csail.mit.edu/medg/courses/6872/2004a/Security+HIPAA.pdf>.28 March 2007
2. Kristina Tarre, "Applied ICT in the Healthcare industry in Sweden-A study conducted by Kristina Tarre on behalf of Invest in Sweden Agency's IT Sweden Project", 19 August 2003
3. Bernard A. Courtois, "the Issue: Health Care", November 15, 2004
4. Pertti Jarvinen, "ON RESEARCH METHODS", OPINPAJAN KIRJA Tampere, Finland
5. Fact sheet, "Swedish health care", Swedish Institute January 2007
6. Luke Davis, Jennifer A. Domm, Michael R. Konikoff, and Randolph A. Miller, MD, Vanderbilt University, Nashville, Tennessee, "Attitudes of First-year Medical Students Toward the Confidentiality of Computerized Patient Records", © 1999, American Medical Informatics Association. Source web address: (<http://www.pubmedcentral.nih.gov/articlerender.fcgi?artid=61344>), 6th, April, 2007
7. Sten Markgren, "Datainspektionen och skyddet av den personliga integriteten", publication, Lund: Studentlitt, 1984
8. Gordana Dodig-Crnkovic, "Privacy and Protection of Personal Integrity in the Working Place", February 2006
9. Mark Weiser, "The technologist's responsibilities and social change". Computer-Mediated Communication Magazine, 1, April, 1995 http://www.ibiblio.org/cmc/mag/1995/apr/last.html; 12, March, 2007
10. Peter Swire* & Lauren Steinfeld**, "Security and Privacy After September 11: The Health Care Example", Minnesota Law Review, Forthcoming Available at SSRN: http://ssrn.com/abstract=347322 or DOI: 10.2139/ssrn.347322
11. Rebecca N. Wright1 and Zhiqiang Yang1 and Sheng Zhong2⋆⋆,"Distributed Data Mining Protocols for Privacy: A Review of Some Recent Results⋆",
12. Thomas C. Rindfleisch, "Privacy, Information Technology, and Health Care", **Communications of the ACM** archive Volume 40 , Issue 8 (August 1997) table of contents Pages: 92 - 100 Year of Publication: 1997 ISSN:0001-0782, **Publisher,** ACM Press New York, NY, USA
13. Latanya Sweeney, "Computational Disclosure Control-A Primer on Data Privacy Protection", 01/08/01 8:22 AM
14. Ministry of Justice of Sweden, fact sheet "Information on the Personal Data Act", Ju 98.05. December 1998
15. Douglas Thomas and Brian D.Loader, "Cybercrime-Law enforcement, security and surveillance in the information age", Publisher: Routledge (13 April 2000), ISBN-10: 0415213266 ISBN-13: 978-0415213264
16. "Customer Success Story: Akademiska Sjukhuset - Uppsala University Hospital" http://www.global360.com/collateral/Akademiska%20Sjukhuset.pdf, 2007-4-15th
17. Glenn R. Simpson, "The 2000 Count: Bureau Blurs Data To Keep Names Confidential," The Wall Street Journal, February 14, 2001

18. Sweden Ministry of Justice, "Personal Data Protection-Information on the Personal Data Act", http://www.sweden.gov.se, 2007/April/28th
19. America National Security Agency, "National Information Systems Security Glossary", NSTISSI 4009 Fort Meade, MD., Sept. 2000
20. W. Victor Maconachy, Corey D. Schou, Daniel Ragsdale and Don Welch, "A Model for Information Assurance: An Integrated Approach", 2001
21. BRADLEY A. MALIN, MS, MPHIL, "An Evaluation of the Current State of Genomic Data Privacy Protection Technology and a Roadmap for the Future", Journal of the American Medical Informatics Association Volume 12 Number 1 Jan / Feb 2005
22. "Public Access to Information and Secrecy with Swedish Authorities", information concerning secrecy legislation etc., REGERINGSKANSLIET
23. The Ministry of Justice, "Public Access to Information and Secrecy with Swedish Authorities", ISBN 91-38-31559-9

English Questionnaire

Approaches towards data privacy in local hospital:(All the opinion will be used **anonymously**) Please choose one alternative or give out your opinion: (Q means Question) X in the box to check it.

Q1. Do you use technique for data privacy/security? No □Go to question3 Yes □ Go to question 2
Q2. What kind of technique do you utilize for data privacy? (Look at appendix1 as a reference, if the technique is not included in the appendix, you can list it in the blank belong as well) _____ _____ _____ Go to question 3

Q3. What kind of approach do you use towards data privacy? (if you have answered Q3, list the other non-technical approaches you use)

Law/Act about data privacy □ Go to question5

Rules in the hospital □ Go to question4

Else_____

_____

_____

Q4. List the most import rules in the hospital about data privacy:

_____

_____

_____

Go to question 6

Q5. What acts/law do you know related to patient privacy? Please list them below:

_____

_____

_____

Go to question 6

Q6 What principle do you follow when you process the patient data for the use of study?

(Processing of personal data includes, for example, collection, recording, storage, adaptation or alteration, compilation or retrieval.[fact sheet, Information on the Personal Data Act, Ministry of Justice])

_____

_____

_____

Go to question7

Q7 What problems do you have with the security and patient privacy aspect? Could you generally list some?

_____

_____

_____

The end

Thank you for helping!!!

Appendix1 Summary of technologies applicable to information system security management.[12]

Intervention	function	Example technology
A. deterrents		
A1.Alerts and reminders	Reinforce user ethics	Vendor-specific
A2.Audit trails	Document access/give alerts	Custom research systems and some vendors
B. Obstacle		
B1.Authentication	Determine who is connecting	Accounts/passwords, Kerberos, tokens (e.g., Secur-ID), public-key systems, biometric systems
B2.Authorization	Define who can access what information	OS file and database vendor access controls, DCE access control lists
B3.Integrity management	Ensure information content is as intended	Cryptographic checksums
B4.Digital signatures	Validate notes and orders	Evolving standards
B5.Encryption	Prevent eavesdropping	PGP, Kerberos, DES, public-key systems, secure sockets
B6.Firewalls and network service management	Define system perimeter and control means of access	Many Vendors
B7.Rights management tools	Control information distribution and access	IBM Crypto-lopes
C. System Management Precaution		
C1.Software management	Guard against viruses, Trojan horses, etc.	Tripwire and controls over loading of uncertified software
C2.System vulnerability analysis tools	Detect unintended system vulnerabilities	SATAN, crack, National Computer Security Association

English Questionnaire-modified version

Approaches towards data privacy in local hospital :(All the opinion will be used **anonymously**) Please choose one alternative or give out your opinion: (Q means Question) X in the box to check it.

Part one

Q1. Do you use technique for data privacy/security? No □Go to question3
Yes □ Go to question 2

Q2. What kind of technique do you utilize for data privacy? (Look at appendix1 as a reference, if the technique is not included in the appendix, you can list it in the blank belong as well)

_____
_____
_____

Go to question 3

Q3. What kind of approach do you use towards data privacy? (if you have answered Q3, list the other non-technical approaches you use)

Law/Act about data privacy □ Go to question5
Rules in the hospital □ Go to question4
Else_____
_____
_____

Q4. List the most import rules in the hospital about data privacy:

_____
_____
_____

Go to question 6

Q5. What acts/law do you know related to patient privacy? Please list them below:

_____
_____

Go to question 6

Q6 What principle do you follow when you process the patient data for the use of study? (Processing of personal data includes, for example, collection, recording, storage, adaptation or alteration, compilation or retrieval.[fact sheet, Information on the Personal Data Act, Ministry of Justice]) _____ _____ _____ Go to question7
Q7 What problems do you have with the security and patient privacy aspect? Could you generally list some? _____ _____ _____ Go to part two
Part two information system security evaluation
Q1 How often you evaluate the information system security? Once in half year □ once in a year □ Else_____ Go to Q2
Q2 What evaluation standard do you follow? _____ _____ The end

Thank you for helping!!!

Matematiska och systemtekniska institutionen
SE-351 95 Växjö

Tel. +46 (0)470 70 80 00, fax +46 (0)470 840 04
http://www.vxu.se/msi/