Information Security Management of Healthcare System

A case study of Blekinge Region Healthcare

KHALID MAHMOOD

ASHRAFULLAH
This thesis is submitted to the School of Computing at Blekinge Institute of Technology in partial fulfillment of the requirements for the degree of Master of Science in Computer Science. The thesis is equivalent to 20 weeks of full time studies.

Contact Information:

Authors:  **KHALID MAHMOOD**  
muqadas@gmail.com

  **Ashrafullah**  
ashrafbth@gmail.com

University advisor:

Dr. Sara Erikson

School of Computing  
Blekinge Institute of Technology

School of Computing  
Blekinge Institute of Technology  
Box 520  
SE – 372 25 Ronneby  
Sweden

Internet : www.bth.se/tek  
Phone : +46 457 38 50 00  
Fax : + 46 457 102 45
Table of Contents

LIST OF FIGURES .................................................................................................................. 5
LIST OF ACRONYMS .............................................................................................................. 6
ABSTRACT ................................................................................................................................. 7
ACKNOWLEDGEMENT ............................................................................................................ 8
INTRODUCTION ....................................................................................................................... 11

CHAPTER 1: BACKGROUND .................................................................................................... 12
1.1 ICT FOUNDATION ............................................................................................................. 12
1.2 ICT IMPACTS AND HEALTHCARE SYSTEM ................................................................. 12
1.3 ICT AND BLEKINGE COUNTY HEALTHCARE PROVIDER ............................................ 13
1.4 HEALTHCARE INFORMATION SECURITY ................................................................... 14
1.5 CHARACTERISTIC OF INFORMATION SECURITY ......................................................... 15
1.6 FUNDAMENTAL COMPONENTS FOR INTEGRATED SYSTEM ......................................... 15

CHAPTER 2: PROBLEM DESCRIPTIONS AND GOALS .......................................................... 17
2.1 RESEARCH QUESTIONS .................................................................................................. 18
2.2 AIMS ............................................................................................................................... 18
2.3 OBJECTIVES .................................................................................................................. 18

CHAPTER 3: RESEARCH METHODOLOGY .......................................................................... 20
3.1 OVERVIEW ..................................................................................................................... 20
3.2 QUALITATIVE RESEARCH METHODOLOGY ............................................................... 20
3.3 LITERATURE REVIEW .................................................................................................... 21
3.4 INTERVIEW ..................................................................................................................... 21
   3.4.1 Top Down Conducting Interview............................................................................. 22
3.5 FRAMEWORK OF METHODOLOGY ............................................................................. 23

CHAPTER 4: THEORETICAL WORK ....................................................................................... 24
4.1 INFORMATION COMMUNICATION TECHNOLOGY (ICT) ............................................. 24
4.2 CHARACTERISTIC AND ROLE OF ICT ....................................................................... 24
   4.2.1 Management System Development ..................................................................... 25
   4.2.2 ICT Integration Support system in Swedish HealthCare ...................................... 26
4.3 INFORMATION SECURITY OVERVIEW ...................................................................... 28
4.4 INFORMATION SECURITY MODEL (SIS CLASSIFICATION) ........................................ 28
4.5 INFORMATION SECURITY OBJECTIVES ....................................................................... 30
   4.5.1 Confidentiality .......................................................................................................... 30
   4.5.2 Integrity .................................................................................................................... 30
   4.5.3 Availability ................................................................................................................ 30
   4.5.4 Authentication .......................................................................................................... 31
4.6 INFORMATION SECURITY EVALUATION MECHANISM ........................................... 31
4.7 ACCESS CONTROL (AVAILABILITY AND ACCESSIBILITY) .......................................... 31
4.8 ACCESS CONTROL CONCEPTS .................................................................................... 32
   4.8.1 Object ......................................................................................................................... 32
   4.8.2 Subject ....................................................................................................................... 32
   4.8.3 Operation .................................................................................................................. 32
   4.8.4 Privileges or Permission .......................................................................................... 32
   4.8.5 Access Control List (ACL) ...................................................................................... 32
   4.8.6 Access Control Matrix (ACM) ............................................................................... 32
4.9 ACCESS CONTROL POLICY AND MODEL .................................................................. 33
   4.9.1 Discretionary Access Control (DAC) ....................................................................... 33
   4.9.2 Mandatory Access Control (MAC) ........................................................................... 33
   4.9.3 Role Based Access Control (RBAC) ......................................................................... 34
   4.9.4 Dynamic, Context-Aware Access Control .............................................................. 34
4.10 ACROSS BORDER (CLIENT-SERVER) COMMUNICATION .......................................... 37
4.11 SECURITY ANALYSIS APPROACH .............................................................................. 37
CHAPTER 5: EMPIRICAL WORK ...................................................................... 44

5.1 CONDUCTING CASE STUDY ................................................................. 44
5.2 DETAILED QUESTIONS ........................................................................ 45
5.3 QUESTIONNAIRE DESIGN ................................................................. 45
5.4 PURPOSE OF INTERVIEW ....................................................................... 45
5.5 INTERVIEW INSTRUMENT ...................................................................... 45
5.6 INTERVIEW REALIZATION ..................................................................... 46
5.6.1 Interview 1 ..................................................................................... 46
5.6.2 Interview 2 ..................................................................................... 47
5.6.3 Interview 3 ..................................................................................... 47

CHAPTER 6: RESULTS ................................................................................. 49

6.1 ACCESS CONTROL PROCEDURE (AVAILABILITY AND ACCESSIBILITY) ......................................................................................... 49
6.2 ELECTRONIC HEALTH RECORDS (EHR) OF BLEKINGE HEALTHCARE ................................................................................................. 50
6.3 LAW, STANDARDS, GUIDELINES OF HEALTHCARE ........................................................ ............................................................. 51
6.4 ACROSS BORDER COMMUNICATION OF SENSITIVE INFORMATION ................................................................................................. 51
6.5 AWARENESS OF INFORMATION SECURITY IN BLEKINGE COUNTY ................................................................................................. 52
6.6 PRIVACY & SAFETY OF PATIENT IN HEALTHCARE IN BLEKINGE COUNTY .......................................................................................... 53

CHAPTER 7: ANALYSIS AND DISCUSSION .............................................. 54

7.1 ACCESS CONTROL PROCEDURE (AVAILABILITY AND ACCESSIBILITY) ................................................................................................. 54
7.2 ELECTRONIC HEALTH RECORDS OF BLEKINGE HEALTHCARE ................................................................................................. 55
7.3 LAWS, STANDARDS AND POLICY IN BLEKINGE HEALTHCARE ................................................................................................. 55
7.4 ACROSS BORDER COMMUNICATION OF SENSITIVE INFORMATION ................................................................................................. 56
7.5 AWARENESS OF KNOWLEDGE OF INFORMATION SECURITY IN BLEKINGE COUNTY ................................................................................................. 56
7.6 PRIVACY & SAFETY OF PATIENT IN BLEKINGE HEALTHCARE ................................................................................................. 56
7.7 DISCUSSION .......................................................................................... 57
7.7.1 Risk Management ........................................................................... 57
7.7.2 Policy and Procedures, Laws and Standards in Blekinge Healthcare ................................................................................................. 59
7.7.3 Unawareness ................................................................................. 59
7.8 VALIDITY THREATS ............................................................................. 60
7.8.1 External Validity ........................................................................... 60
7.8.2 Construct Validity .................................................................... 60
7.8.3 Internal validity ................................................................ 61
7.8.4 Conclusion validity ................................................................... 61

CHAPTER 8: EPILOGUE ............................................................................... 63

8.1 RECOMMENDATIONS ........................................................................... 63
8.1.1 Risk Management and Risk Assessment ............................................. 64
8.1.2 Information Security Management System (ISMS) ........................................................ ........................................................ 64
8.1.3 Awareness and Advocacy ................................................................... 64
8.1.4 International Constitutional Legislative Acts ........................................ 64
8.1.5 Access Control ............................................................................. 65
8.1.6 Dynamic—Context Role Base Access Control (DRBAC) ....................... 65
8.1.7 Logging Management with Error control ............................................ 65
8.1.8 Standard Software and Hardware .................................................... 65
LIST OF FIGURES

Figure 1: Health care management System
Figure 2: Organization of Swedish Health Services
Figure 3: Health Care Network Security
Figure 4: Research Question Designation with Aims, Objectives and Outcomes
Figure 5: Information Society Evolution Stages
Figure 6: Evolution Management System
Figure 7: Six Action of Swedish Healthcare Plan
Figure 8: Information Security Model of SIS 2003
Figure 9: DRBAC
Figure 10: Client and Server Communication Path
Figure 11: Information security management system (ISMS)
Figure 12: The six Acts that cause an impact on healthcare
# List of Acronyms

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Full Form</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACL</td>
<td>Access Control List</td>
</tr>
<tr>
<td>ACM</td>
<td>Access Control Matrix</td>
</tr>
<tr>
<td>ARRA</td>
<td>American Recovery and Reinvestment Act</td>
</tr>
<tr>
<td>CDSS</td>
<td>Clinical Decision Support System</td>
</tr>
<tr>
<td>CIA</td>
<td>Confidentiality, Integrity and Availability</td>
</tr>
<tr>
<td>DAC</td>
<td>Discretionary Access Control</td>
</tr>
<tr>
<td>DHHS</td>
<td>Department of Health and Human Services</td>
</tr>
<tr>
<td>DRBAC</td>
<td>Dynamic Role Based Access Control</td>
</tr>
<tr>
<td>EHR</td>
<td>Electronic Health Records</td>
</tr>
<tr>
<td>EPHI</td>
<td>Electronic Protected Health Information</td>
</tr>
<tr>
<td>EPR</td>
<td>Electronic Patient’s Records</td>
</tr>
<tr>
<td>HIPPA</td>
<td>Health Insurance Portability and Accountability Act</td>
</tr>
<tr>
<td>ICT</td>
<td>Information Communication Technology</td>
</tr>
<tr>
<td>IDSS</td>
<td>Intelligent Decision Support System</td>
</tr>
<tr>
<td>IPC</td>
<td>Inter-process Communication</td>
</tr>
<tr>
<td>ISMS</td>
<td>Information Security Management System</td>
</tr>
<tr>
<td>IT</td>
<td>Information Technology</td>
</tr>
<tr>
<td>MAC</td>
<td>Mandatory Access Control</td>
</tr>
<tr>
<td>NHS</td>
<td>National Health Service</td>
</tr>
<tr>
<td>NPIT</td>
<td>National Program of Information Technology</td>
</tr>
<tr>
<td>NSTISS</td>
<td>National Security Telecommunication and Information System Security</td>
</tr>
<tr>
<td>OS</td>
<td>Operating System</td>
</tr>
<tr>
<td>PDCA</td>
<td>Plan DO Check Act approach</td>
</tr>
<tr>
<td>PHI</td>
<td>Protected Health Information</td>
</tr>
<tr>
<td>RBAC</td>
<td>Role Base Access Control</td>
</tr>
<tr>
<td>SSL</td>
<td>Secure Socket layer</td>
</tr>
<tr>
<td>VPN</td>
<td>Virtual Private Network</td>
</tr>
</tbody>
</table>
Information security has significant role in Healthcare organizations. The Electronic Health Record (EHR) with patient’s information is considered as very sensitive in Healthcare organization. Sensitive information of patients in healthcare has to be managed such that it is safe and secure from unauthorized access. The high-level quality care to patients is possible if healthcare management system is able to provide right information in right time to right place. Availability and accessibility are significant aspects of information security, where applicable information needs to be available and accessible for user within the healthcare organization as well as across organizational borders. At the same time, it is essentials to protect the patient security from unauthorized access and maintain the appropriate level in health care regarding information security.

The aim of this thesis is to explore current management of information security in terms of Electronic Health Records (EHR) and how these are protected from possible security threats and risks in healthcare, when the sensitive information has to be communicated among different actors in healthcare as well as across borders. The Blekinge health care system was investigated through case study with conduction of several interviews to discover possible issues, concerning security threats to management of healthcare. The theoretical work was the framework and support for possible solutions of identified security risks and threats in Blekinge healthcare. At the end after mapping, the whole process possible guidelines and suggestions were recommended for healthcare in order to prevent the sensitive information from unauthorized access and maintain information security.

The management of technical and administrative bodies was explored for security problems. It has main role to healthcare and in general, whole business is the responsibility of this management to manage the sensitive information of patients. Consequently, Blekinge healthcare was investigated for possible issues and some possible guidelines and suggestions in order to improve the current information security with prevention of necessary risks to healthcare sensitive information.

**Keywords:** Information Security, Electronic Health Records, Information Communication Technology, patient privacy and security
ACKNOWLEDGEMENT

In the name of ALLAH, the most gracious, merciful and creator of the universe. We are grateful to ALLAH who blessed us with abilities and strength to do this thesis work on time. We are thankful and admire the untiring support of our supervisor Dr. Sara Erikson. It was through the guidance and support of our supervisor that helped us in making this thesis work a reality.

We express our gratitude for all our Family Members, for providing their untiring support and prayers during this thesis work. We are thankful to our colleagues Mr. Muhammad Ullah, Mr. Farrukh Sahar, Mr. Falakzeb Khan, for extending and sharing cooperation, knowledge and experience with us. Who encourages us to do this thesis work? They all supported us whenever we were facing problems and struggling to achieve our goals.

We are also especially thankful to all healthcare personnel, who gave us constructive, useful suggestions and valuable feedback.

From KHALID MAHMOOD, a special word of appreciation for my Siblings for being the reason of my achievements here at Blekinge Institute of Technology. This thesis is dedicated to my Parent, whose prayers are always with me in every sphere of my life.

At the end, we are especially thankful to SWEDEN and Swedish people for providing us the opportunity with high quality of education.
INTRODUCTION

The information of patients in the form of Electronic Health Records (EHR) or patient electronic journals is the most important information of healthcare organizations. The citizens of county endeavor to get high quality care from healthcare providers. It is thus necessary for healthcare management to have some well-organized structure or form to manage the patient’s information and Electronic Health Records (EHR) data in system. The existing information and data of patients in healthcare can be classified as sensitive to manage. Well-organized structure of sensitive information in healthcare management system aims to provide good opportunities of care based upon the right information to right place in right time [51, 58].

Figure 1: Information security management provide right information to right place in right time to right person

Figure 1 depicts as example that information security management system should have all possible information with resources, which are required to obtain a high quality health care of patients and good quality health care. It is possible if ensure to have high-level information security for system to have right information to right person in right time to right place. The healthcare organization does not have sufficient information about patient’s treatment or this is unavailable to management, this way lead to inappropriate treatment of patients. The sensitive information of patients in healthcare is managed in a computerized based environment, therefore for better protection high-level requirements and needs concerning security are required. Moreover, an electronic based healthcare system increases the availability, accessibility and ease of use of information and resources. The electronic based management system endeavors to manage the information according to stakeholder’s requirements in several ways. The users should be able to access their information or Electronic Health Records (EHR) across borders organizational through electronic based information system. Implementation of Electronic Health Records (EHR) in health care has increased the high quality treatment of patients. The development of electronic based system
and implementation has been beneficiated healthcare for management but on the other hand, it is a potential security threat and risk to management. Therefore, the potential security threats to sensitive information in healthcare violating the patient privacy and patient security [51, 58].

Blekinge County is situated in the south east of Sweden. The configuration of healthcare public sector in Sweden is organized on national level, regional level. Blekinge Health Care is run by county council and has the sensitive information of patients and providing high quality of treatments to citizens. Electronic based infrastructure has been using since long time for quality treatment to county citizens. The county citizen records are stored electronically in healthcare and provided to actors electronically inside but the traditional way of transmission is papers based across border healthcare. The traditional transmission way, which is paper bases, is insecure method for communication across border for treatment purpose because it does not always guarantee the right information to person in right time. Regarding patient privacy and patient security, both technical and administrative bodies are important factors of information security model to prevent from unauthorized access in order to secure sensitive information [58].

Authors have chosen this research after studying of number of information security related articles and research papers concerning different areas. Healthcare is one of the important areas because it has sensitive information and these resources should be available and accessible to users in order to support of high quality treatment but other hand it is necessary to ensure high-level security for the information.

We have read literature to obtain a better understandable of effective management of information of security in different areas. To explore properly how it is working, to what extent the health care system is satisfied within existing information security application and resources today. In addition, does the existing development fulfill the security requirements, standards and needs of health care organizations? Our research methodology was to conduct several interviews to know the existing information security approach in healthcare and whether it fulfills the security requirements of management. General case study was conducted to discover more how the system actually works. After analyzing the current information security structure of Blekinge health care, we have proposed some recommendations, guidelines. Hopefully, the proposed suggestions will be able to enhance the information security to sensitive information of health care. High level of patient security would be possible to obtain in electronic based healthcare system while still effecting availability and accessibility. The management properly will use the resources through secured way in order to maintain Confidentiality, Integrity and Availability (CIA) [51].
STRUCTURE OF THE THESIS
The structure of the thesis is as follow.

Chapter 1 (Background): It is about the background of the topic. Where the authors explore concept of ICT implication with information security in healthcare provider organizations.

Chapter 2 (Problem Definition/Goals): This chapter discusses relevant problems regarding information security in healthcare provider organization. The authors have presented the research questions about specified domain with expected aims and objectives.

Chapter 3 (Research Methodology): It is about research methodology. This chapter explains the literature review, the approach of interview. That is conducted according to specified domain of interest.

Chapter 4 (Theoretical Work): This chapter is the main part of domain of interest. This chapter discusses the structure of ICT in healthcare. The information security model is explained. Different techniques of information security for healthcare provider organization are discussed. The number of information security characteristic was discussed to ensure the information security for organization. Access control with international standards and legislations acts were explained for security purpose.

Chapter 5 (Empirical Work): This chapter discusses empirical study of this research. The details questions were designed before for conducting interview from healthcare personnel. The designed questions were asked about our domain of interest from Blekinge healthcare provider. Different personnel were selected for conducting the interview. The simple case study was also conducted just to overview the current system of this county.

Chapter 6 (Results): This chapter describes the possible result, where the authors have achieved from interviewees personnel of Blekinge healthcare provider. The focus was the access control, electronic health record, laws, standards and guidelines. This part also discusses the communication of information across borders.

Chapter 7 (Analysis and Discussion): The result from chapter six were discussed and analyzed in this chapter. The conclusion regarding information security was explained in this chapter also.

Chapter 8 (Epilogue): This chapter is included of the recommendations of research study. The conclusion and future work of this study (management of information security) are discussed.
CHAPTER 1: BACKGROUND

In this chapter, the authors have focused the Information Communication Technology (ICT) scope and impacts in healthcare provider’s organizations. In addition, the information security regarding ICT discussed. We know that number of organizations depends on the ICT based structure. The main purpose of ICT is to make cost effective and well-organized environment in organizations [1].

The important role of ICT is the facilitation of accessibility to resources in organizations. Furthermore supporting and enhancing the knowledge of the users and supporting communication between users. The implementation of ICT has provided a framework for access and utilization of resources [2].

1.1 ICT Foundation

These are the following foundation of ICT.

a) Informatics: Informatics has to explore the area of computer science with evaluation, realization, processing system for information, S/W, H/W and aspect of human beings [2].

b) Informatics Technology: IT has to deal with the applications related technological aspect of informatics [2].

c) Information and communication technology: it deals with the combination of informatics technology and communication technology and as a result defines the approach of ICT [2]. Information Technology and Communication Technology with applications have cost-effective approach, faster information transportation [6].

Knowledge management has to identify in term of ICT the enhancement of knowledge sharing and the improvement to access the required information concern and about to knowledge. Sharing the knowledge relatively is concerned to communication. Further, the suggestion of management is the information distribution of knowledge among different factors in organization. Therefore, for management system having ICT infrastructure, the operation of internal and external knowledge sharing has to impose what kind of knowledge and its strategy in order to recognize properly the flow information in organization. For this purpose, ICT has developed a structure to keep the flow of information well organized, less time consuming and to make available the resources [3].

1.2 ICT Impacts and Healthcare system

Information is important for organization. There is vital role of Information communication technology (ICT) in Healthcare providers. A health care provider is preventive care to provide a stay for the patients for treatments. Moreover, patient’s concern to medication information and journals should secure and protect. It is expected commonly that patients e-
journals and concerned information about patients in health care system are produced, modified, transferred, intercepted and stored daily [4].

ICT based healthcare provider organization to make sure the well-organized structure of whole process of communication among users with activities in system i.e. electronic health records or electronic patient records. The Electronic Patient’s Records (EPR) and patient’s electronic journals are communicated among different users in Healthcare organization, which is common concept of human beings that it could be stored to repository [5].

Health care providers’ organization has grown up largely through the development and wide contribution of ICT and adopted the shape of large sensitive information industry. The ICT based health care system has following wide range of enormous opportunities for optimization i.e. enrichment of services, expenditure cost reduction, controlling mechanism, sophisticated management system, supply chain management, electronic scheduling management, information management improvement, various tool specified for different clinical purpose, Clinical Decision Support System (CDSS), Intelligent Decision Support System (IDSS) and monitoring and prevention through (CDSS)[6].

Number of stakeholders and variation of activities of actors are involved in health care system to have strong relationship with each other and together utilize the technology with applications for different kind of purpose. While shared interrelations among different stakeholder in healthcare using different application bring them to work and process the communications [6]. The flow and communication of high sensitive Information of E-journals and EHR and among different stakeholder in health care system must be secured and safe from unauthorized users to access. Regarding of retrieval information and activities of actors causes difficulties to management system to identify apparently, what kind of communication distribution is being retrieval.

The National Health Service (NHS) of England is public organization and given certain targets of health care services to be carried out soon including the implementation of National Program of Information Technology (NPIT). There were certain amounts of services of (NHS) i.e. the Electronic Patients Records (EPR), electronic scheduling, electronic prescribing and broadband communication [9].

1.3 ICT and Blekinge County Healthcare Provider

The Blekinge County is a coastal area of Sweden geographically situated at south east of Sweden. This County is characterized by its smallness and surprising variety of beauties. Accordance to 2008 estimate more than 150000 inhabitants is living in Blekinge County while the total area of this county is 2941 square Kilometer. The county council has the responsibilities to provide the basic infrastructure of health services and support the people to promote the education of health care, such environment to contribute e-health structure in county with the support of wide-ranging installation ICT on priority basis. Other hand, the individual of that county has equal and substantial access to health care facilities according to their requirements and desires [10].

Currently that county has implemented various ICT areas with electronic based applications. Since earlier through the support of National strategy of e-health Sweden, the hospital does provide these services to patients to provide high-quality care, reliable services quickly. The electronic patients journals and electronic health records (EHR) of health care is important
factors of ICT area and should be used as initiatives for security of sensitive records and information communication within in system[11,12].

Figure 2: Organization of Swedish Health Services [11]

### 1.4 Healthcare Information Security

Healthcare system infrastructure i.e. users has lot of dependencies on existed information and mainly information does address the valuable assets for health care. Therefore, patient’s electronic journals, electronic health records (EHR) have a vital role in healthcare and must be secured and appropriate safety from unauthorized users. In addition, the whole communication process of users in health care in a sequence to perform specific targeted task must be secured and safe [4].

Getting better security of patient’s information, the information security must be able to significantly to classify the confidentiality of patient’s information and further extending the security measures successively in same system [7].

In healthcare provider organization has the information risk management is primary approach used for security purpose to meet the requirements of health care regarding mitigating risk and attempt to provide the high level quality care and well organized infrastructure to patients with good security [8].

The American Recovery and reinvestment act of 2009 (ARRA) has developed a few classification to secure the sensitive information and data of health care. This was Protected Health Information (PHI) and usually distributed in different health care providers to make sure the protection of sensitive information communication flow of unauthorized access, which causes the security risk to management. The target of this approach is to find out all kind of illustrations of confidential data and must be providing separate controlling area to observe the communication circumstances against security risk [8].
1.5 **Characteristic of Information Security**

The concept to improve the information security of health care provider organizations, some points should be emphasized effectively to achieve safety/privacy of patient’s electronic journals and electronic health records. During the processing of any information among stakeholders of healthcare providers, the information security is the main requirements to have properties of CIA. Following are basic characteristic to fulfill the security requirements and needs [14].

- **Availability:** Right requests or resources must be done at right time and at right place
- **Integrity:** Do not have permission to change
- **Confidentiality:** Do not access to unauthorized users
- **Accountability:** Individually differentiate the operational performance regularly

1.6 **Fundamental Components for Integrated System**

Encapsulation collections of all components in system make up system functionally. That encapsulation collection of all components works in term of layer in organization. In addition, multilayer in system needs significance security. Following are fundamental components to define a complete system having all kind of possible properties to run the system [13].

- **Component or products**
- **Operating system and communication resources with all kind of things to define a complete structure of organization**
- **Applications**
- **Information Technology personnel**
- **Internal users and management and administration**
- **External users or customers**
- **Surrounding environments**
Figure 3: HealthCare providers Security
CHAPTER 2: PROBLEM DESCRIPTIONS AND GOALS

Electronic Health Record (EHR) with patient electronic journals in the health care system has a key role. Every day a great number of patients are in interaction with doctors, nurses, pharmacists, other healthcare workers, and the relevant information about patient’s medication or journals are communicated among different actors or users in health care system. Therefore, there should be an appropriate and well-organized structure/mechanisms for storage, effective management and securing such information against threats. Through Information and Communication Technology (ICT), development has clearly contributed in health care system but meanwhile the threats to electronic information increase simultaneously. It is worth considering that the effective management of such information is another challenging issue in terms of security threats [4].

Mostly the generic security problems considered in health care information systems concern technical and administrative security paradigm. While the administrative level has less participation as compared to technical security and ensuring strategies, policies etc. also the technical security in health care has a vital role. Basic information security problems in both above domains can be threats, risk, crimes and access control issues [25].

Because the sensitive information of the patients is transformed and translated among various actors in organizations or cross border, the information of electronic health records or patient’s information becomes more vulnerable due to transportation of information. This can be due to deficiencies both at technical and administrative level. In addition, most of the users/actors have inadequate security training, insufficient security education, and lack of knowledge and unawareness of technical security, which can lead to more error prone system.

Furthermore, in the healthcare provider system, many different standards of both software and hardware create considerable issues in terms of security, when it comes to data processing, storage and retrieval. Therefore, in health care system, the sharing of information is a non-negligible security risk. Thus, the flow of such information among different clients or across different borders needs to be secure and reliable in term of availability in order to insure an acceptable health care system for normal user. Secondly, every stakeholder in healthcare organization should have enough information security education, and sufficient knowledge to understand the potential vulnerabilities, which exist in a system versus either insiders or outsiders. There should also awareness to all actors about security of information, resources they are using and the way of transactions take place [25, 58].
2.1 Research Questions

1) What are the problems in information management in the investigated area regarding Information security?

This research question will lead us to investigate the different limitations that can be found when it comes to the information security of the investigated area. We will identify and explore the shortcomings while going for information security (confidentiality, integrity and availability). This will also force us to identify information management challenges in terms of security of information and will provide knowledge, which will be useful for the second research question.

2) How these problems can be solved to improve information security?

The question is addressed through a qualitative approach, by conducting a literature survey initially, followed by interviews and case study. The outcomes of this question will provide different solutions and guidelines for improvement of information security.

2.2 Aims

The aim of this thesis is to identify and analyze the security threats that do exist for Electronic Health Records health care system in the investigated area. Based on identified and analyzed security threats in literature and the outcomes of the interviews, recommendation and guidelines will be offered.

2.3 Objectives

The objectives of this research will be to meet the requirements and needs of our aims. For this purpose, the existing management system of information security of Blekinge healthcare provider will be investigated to obtain the current information system regarding Electronic Health Records (EHR) to ensure the patient security.

Objective 1:

To identify the security problems that exists in the management system of Blekinge health care environment regarding patient security. In most, cases the problems of information security to management system Blekinge health care will be identified according to the requirements and needs of information security.

Objective 2:

How the management system of electronic health records (EHR) to explore and map Blekinge HealthCare with deals these security issues based on information security requirements and needs.
Figure 4: Research Question Designation with Aims, Objectives and Outcomes
CHAPTER 3: RESEARCH METHODOLOGY

Different types of research methodologies are available. For example qualitative, quantitative and mixed methodology [15].

In this chapter, we present our research methodology. The authors have used the qualitative research methodology. In our research, the literature study according to information security was conducted to collect different materials or data about our research area. The literature study was been carried out in order to get a deeper understanding of concepts and even start of the art in research in this area. Further, the case study was conducted to kno problems and issues, which have not been extensively yet in this area. The case study within organization, the approach of interview is the most important method to gather relevant information about specified domain [17]. The authors have conducted the top down interview from different personnel of Blekinge healthcare providers in order to get different opinion regarding in this area.

3.1 Overview

Our research was completed through different phases. First, we have to carry out a literature review concern in our particular domain. The authors have tried to extract those results, problems and issues from available literature. Based on the literature review, the general as well as specified study about our domain was performed. We have been leaded by the literature study to find out gap in our research area. In these gaps, the role of Information Communication Technology (ICT) and its structure in healthcare provider system would be highlighted for the implementation of better security structure. The proper security structure of health electronic records was analyzed.

In this research, the authors conducted the interviews from users of Healthcare provider organization to acquire the details description and knowledge of information security of electronic health records and patients e-journals through details questions. After conduction the interview, the findings of interview was analyzed and discussed to attain the appropriate solution for our objectives.
We have chosen a qualitative research methodology to collect the materials and that collected information was analyzed to understand the requirements of gap of this current research in this area.

3.2 Qualitative Research Methodology

In qualitative research, the authors gathered knowledge in order to understand phenomena and to know that what kinds of reasons are behind events. The attitudes, experiences and opinions of the research participant are especially in focus in qualitative research [17].
There are different types of qualitative research.

| Interviews | Gathering qualitative oral or written response of participant about opinions, facts, and behavior attitudes experiences. |
| Content Analysis | By deconstructions of written, visual and oral, narratives. |
| Focus group | Group of participants discuss specified or told idea or topic usually supported by a moderator. |
| Observation Participatory design | Observing and make recording of such behavior and preferences, which is analyzed in order to explain obviously criteria developed by the researchers. |
| Usability test | Gather information from products, visibility testing of products and services. |

Table 1: Examples of Qualitative Research [17]

3.3 Literature Review

The authors have done a literature review of the selected domain of interest. Literature review is a methodology to investigate the concepts of a domain according to existing theoretical find the key areas of domain of interest. Simultaneously a literature review is an excellent way to collect appropriate resources about information security of Electronic Health Records (EHR). Inclusively the literature review is to extract appropriate findings or contexts of investigated research from previous research papers or articles, extensive and relevant knowledge is provided to support the researchers [18].

Usually the literature review pertains and relevant to those materials, which were written in web references, articles and books [16]. To identify central concept within of our domain of interest more clearly number of searches were carried out mainly using digital libraries and search engines such as IEEE explore, ACM digital library, Google, yahoo and web search engines etc [16].

As with the management, information security is the domain of interest of research area, from number of research papers, the relevant materials were extracted. The literature review helped us to determine and delimit our domain area.

3.4 Interview

After completion of the literature review combined with an informal discussion approach, the authors have decided to conduct interview. In case studies, face-to-face meeting is essential to gather information within organizations [17]. To investigate the information security issues of electronic health records (EHR), the authors have conducted several interviews with employees in health care system of Blekinge County.

Different actors involved in health care system were interviewed in order to gather qualitative data about different activities and attempt to identify possible deficiencies or
shortcomings in terms of information communication technology (ICT) in health care. Three different interviews were conducted with different stakeholders of health care in Blekinge County. These included top-level administration and management, Doctors and technical administration (IT staff). The author conducted pre-planned questions to ask about the management of information security of healthcare provider. During the interview, some questions were posed to investigate the specified domain thus including informal discussion or questions. The interviews were recorded to make the ensuring analysis simpler, and we took notes during the interviews.

### 3.4.1 Top Down Conducting Interview

In Blekinge County to conduct the interview from different stakeholders in health care, we have used the top down conducting approach. In health care organizations, numbers of levels are to be dealt with for different business and dealings.

The top-level interview that is top management and administration of healthcare provider was conducted first for the interviewing purpose to extract the information of management and how the strategy of this area is beneficial for entire information communication system. After top level of management, the authors contacted the Doctor for conducting the interview related to information about availability, security, access control and reliability of Electronic Health records and including overall resources for ensuring safe and harmless treatment etc. Finally, the management, responsible for handling the IT staff was interviewed. In this level of contact deep investigation and interview was conducted to know how the management of ICT or IT staff understands to provide the security of information.
3.5 Frame work of Methodology

Phase 1
- Literature Review
  - ICT
  - SECURITY
  - EHR

Phase 2
- Case study
  - Design questionnaire
    - Interview
  - Admin/Management
  - Medical Staff
  - ICT and security
  - Interview result

Phase 3
- Conclusion and Result
  - Analysis
  - Discussion
  - Conclusion
CHAPTER 4: THEORETICAL WORK

This literature review focuses on information security of patient’s information in the form of Electronic Health Records (EHR) used by healthcare providers, how to maintain the information security of Electronic Health Records in healthcare organizations. In healthcare organizations, the information of patients is transmitted for communication among various actors or sometimes it is transmitted across border. The focus of this work is to evaluate the security risk in healthcare sensitive information when and where it does exist when the data is communicated in system and what mechanisms are used for managing the system in order to reduce the risks.

Furthermore, we aim to explain the implications of information communication technology, briefly the integrated management system developed through ICT, information security and its different characteristics. In literature review, the focus is information security model for healthcare providers to enhance the information security. Different kinds of international standards, guidelines and Swedish healthcare legislative acts to enhance the information security are discussed.

4.1 Information Communication Technology (ICT)

Information Communication technology is not only hardware and software applications but also it is about dealing with designation, implementation, development, support and management of computer based information systems. ICT is known electronic based system or computer based system and has the properties of transmission and communication of information, procession, storage, and retrieval of information. The ICT approach not only deals with retrieval of information, storage, processing and communications of information, transmission but also some times deals with protection of information. Since many years the rapid development and diffusion of ICT in different organizations has brought informational communication and transmission revolution in the world. Sharing and transmitting information via ICT among organizations independent of their location has made the world likely a global village [19].

4.2 Characteristic and Role of ICT

Increasingly merging global culture is facilitated by technology. The growing ICT has brought people together and is integrating the entire infrastructure of many systems simultaneously [20]. The knowledge management has categorized the sharing of knowledge. Knowledge is the soft combination of data, information, knowledge and wisdom to give a better understanding of something. Core knowledge when it is transmitted among several organization focuses on the information communication technology [21]. Nowadays ICT is considered a foundation in an organization and has a distinctive role in an organization like health care to deliver better relevant and appropriate services to users [4].
According to figure 5 the ICT development Index indicates that improvement and strengthening of ICTs in information society has come through different stages and adopted the shape of technological development. This technological development through different stages aims to develop the information society is related to ICT [22]. There are different aspects of ICT in organization to enhance the services i.e. processing, repetitive aspect, searching, data storage capacity and data communication. These aspects are functioning properly in system through various ICT related factors like reliability, durability, efficiency, flexibility etc [41].

Information Communication Technology is like an umbrella term for the technological purpose, which is generated through the combination of computer technology with communication [23].

4.2.1 Management System Development

The integrated management system is developed by implementation of ICT to facilitate different resources in system in order to fulfill the requirements of management. According to (ISO, 2000) explanations, the sustainable management system anticipates what and how the organizations manage the entire processing, activities of resources and performance so aim is to achieve the objective of services and resources[24].

In 2007, Kerstin Dahlgren Persson presented a model to represent performance of the system in organization because the integrated systematic management system was implemented to perform the activities in organizations to get better performance [24].
The integrated management system provides support concerning issues related to performance, safety, quality, security and health with aims to address the possible achievement of objectives. It provides a way of delivering the image of a top-level management system with the required objective of the organization.

In case of IAEA, the integrated management system provides the safety standards. A safety standard has to define some requirements, and then it presents the guidelines regarding implementation, accessing, and establishing to improve the integrated management system. The improved management system has the integration of following elements: health, quality, security, environments, and safety, and maintains the proper safety performance among all activities in the organization [24].

4.2.2 ICT Integration Support system in Swedish HealthCare

According to Swedish national strategy for E-health, the figure 7 represents the integrated ICT support system for Swedish health care. The Swedish ICT is based on support system with social services with mutual coordination at number of levels. Figure 7 depicts six different actions area represents as a group with coordinated measures. The web-based application or portal is required by the patients and placed at the highest level to get information about health, advice, and services. After the highest level, the centralized system is required to professional of health care in order to achieve all relevant information system. Here the important elements are (EHR), DSS, Administrative support system and patient summary. Infrastructure support services are important aspect of Swedish health care system related to technical area and ensure some activity of effective security and some tools related to communication networks. At the end, standards and regulatory framework are concerned to information structure and laws and regulation respectively are fundamental structure to support the ICT environment [11].
Accessibility internal portal
- Health information
- Advice
- Services

Information system and process support
- Electronic Health Record (EHR)
- Administrative support system
- Decision Support system
- Prescription support
- National patients summary

Infrastructural support system
- Communication network
- Electronic directory
- Identification
- Authentication
- Handling consent
- Logging
- Information structure

Standards

Regularity Framework
- Laws and regulation

Figure 7: Six Action of Swedish Healthcare Plan [11]
4.3 Information Security Overview

In the perspective of information technology, the concept of information security is become more pervasive and increasingly used. The information security has to deal with that information to be protected from access of unauthorized users [25]. In 2003, Swedish standardization of information technology (Swedish standards institute SIS) has introduced some concerns of information security to make sure the protection and safety of information assets. The main purpose of the Swedish standardization of information technology is to continue the support of integrity, availability, accountability and confidentiality and protect the sensitive information availability in system. How to suggest to secure the important information or records in organization so the different terminology of information security is available and mainly focus onto organizations requirements to select the information security mechanism. The available and implemented tools in organization, management have the responsibility to manage the sensitive information secure appropriately in system from unauthorized disclosure. According to Swedish standardization of information technology (SIS), IT security and data security are associated and relevant to form the information security [25].

Data security: The term data security is protecting the computer systems with its data. IT security: The Information technology security protects the IT system with its data Information security: Information security is defined to protect the information resources or assets.

4.4 Information Security Model (SIS Classification)

The above (SIS) conceptual classification of security we have to explain the information security model to define the different security measures and containing the following characteristic of information security to provide the good way for processing of information in organization. These characteristics are integrity, availability, confidentiality and accountability [25].

INTEGRITY:
According to information security, the integrity concerns to that information or data could not be changed without authorization. Prevention of unauthorized modification and fabrication of system sensitive information [14, 34].

AVAILIBILITY:
It is the assurance where the system is responsible to store, deliver, processing of information so these are accessible to those right person who are authorizer. Other hand availability is to concern to those information that are accessible to right person, at right place and at right time [14, 34].

CONFEDIALITY:
This key concept of information security pertains how to prevent the information of organization from unauthorized disclosure. They have to impede the unauthorized users from
accessing sensitive information of organization. It is the assurance of that information that are only to accessible and share among authorized users or also organizations [26].

ACCOUNTABILITY:

The accountability is defined in information security perspective that the individually authentication and identification of the users maintains the accountability [44].

As well to information security model proposed by (SIS 2003), at the top level it exits the characteristics of the information security while below information security is followed by the security measures. In information security model both, the administrative and technical securities are placed on organization level to achieve the goals of these four characteristic.

The management elements like tools, policies, strategies, risk assessment and risk management are concerned to administrative security. On this level, the technical security is to be obtained to accomplish all technical related requirements and further it is divided into two different parts. One is called IT security and other is Physical security. The physical security protects the physical information in organization for example the system of alarm and fire while IT security of Technical security has concerned with technical information system. Furthermore, the computer security and communication security are subparts of IT security. Number of Hardware and its contents are protected by the computer security while the business of communication security is to make sure the protection of networks and way where the information and communication are transmitted among different system or nodes is called the communication security [25].

Below figure depicts that all requirements are related to information security characteristics of organization must be performing the achievement regarding to information security [25].

Figure 8: Information Security Model of SIS 2003[25]
4.5 Information Security Objectives

Information security is technology dealt with protecting the different information resources and system information from unauthorized access. In organization, there is a flow of communication of information among the clients to perform the required task so all procession of resources in system is brought by the interconnected network system [27]. Therefore following different area is corresponding to threats to Information Technology security (IT) [34]. Users as regarded to access the records, disruptions, disclosure, modifications. According to our study, we will focus or concentrate on the following key concepts of information security of information

1. Confidentiality
2. Integrity
3. Availability
4. Accountability
5. Authenticity

4.5.1 Confidentiality

This key concept of information security pertains how to prevent the information from unauthorized disclosure. They have to impede the unauthorized users from accessing the sensitive information of system. It is the assurance of that information that are only to accessible and share among authorized users or also organizations.

In health care information system, the sensitive information like electronic health records (EHR), patient’s prescriptions, patient’s e-journals should be provided privacy (usually related to personal data) and secrecy (usually related to organization information) in order to protect the assets of patients as well as organization from unauthorized users [26]. Numerous concerns to security have been identified and concentrated on identification, authentications and authorization (confidentiality) [28, 34].

4.5.2 Integrity

Prevention of unauthorized modification and fabrication of information in organization. According to information security, the integrity concerns to that information or data could not be changed without authorization [14, 34].

In health care system the integrity and privacy of the users or patients is utmost significant in order to protect the sensitive information or (EHR) of patients from unauthorized users to make modification. In addition, the information integrity is called the trustworthiness of information in organization to provide on demand the reliable, consistent and accurate data or information about patients or information related to organization. [29, 30].

4.5.3 Availability

It is the assurance where the system is responsible to store, deliver, processing of information so these are accessible to those right person who are authorized. Other hand availability is to concern to those information that are accessible to right person, at right place and at right time.
This term is concerned to information property of any system and on demand accessible to users through reliable authorization. According to availability of information security to make sure the right access of users that, required sensitive information would be available to authorized users. For example, the sensitive information of any concern should be available to right users at right time and at right place [34].

In health care organization the electronic health records or e-journals of patients is sensitive information and it may deal with sensitive data of system to provide the right information at right time when it has been needed to right place [31, 26].

4.5.4 Authentication

The authentication deals with transmission and communication of information with legitimate users. The involvement of this kind of measures is to prior identification of any subject and after verification, the subject has provided the accessibility to get the required information. Conventionally authentication process of information security is aiming to verify something, as you have to know. Something you have and something you are [26]. HIPPA is organization for standards and explained the policies with procedures for authentication purpose of individuals in organizations. We know that authentication has to play the front line security, which are often user names with passwords in multiple organizations is trend of authentication [40].

4.6 Information Security Evaluation Mechanism

Following are the several mechanisms used by management to protect the individuals and collective sensitive information from vulnerabilities or found the risk and threats to information [32]. In our thesis, we will focus on the risk management and access control to ensure how long it evaluates better the security threats to sensitive information of healthcare.

- Risk management
- Firewall & Connectivity Management
- Encryption
- Password Management
- Authentication and access control
- Fallback planning
- Monitoring & intrusion detection
- Virus prevention & Detection
- Infrastructure security management
- Physical security

4.7 Access control (availability and accessibility)

In organization, it is the primary responsibilities of top management to have satisfactory security of information as well as information system. Those applications in organization usually deal with safety and privacy has included the access control. Access control is a mechanism of information security to determine the allowed resources or objects (access control list) in organization to legitimate subjects (users). Access control is mediating every attempt of subjects or users in organization to access control list (objects). After successful process of authentication and verification in organization, the comprehensive accesses are granted to verified users. Usually organization management planning is to implement the approach of access control in system. It should be considered in organization at different level of abstract i.e. access control policies, models and mechanisms [45].
The fundamental objective of the access control in information system organization is appropriately protecting the resources of system from inappropriate users and make sure the availability of information to both users and application [45].

4.8 Access Control Concepts

This section of access control concepts introduces some basic concepts.

4.8.1 Object

It is the entity of access control to contain about the information or resources or contains the receiving information. Usually access to object of control access means to access potentially the contained information or resources i.e. in database records or fields, files, directories, process and programs. Additionally processors, printers, nodes of networks, video displays and different components are the objects in system [45, 46].

4.8.2 Subject

It is the entity of access control included of personnel, users, process and devices etc. the function of subject in system is to flow the information among objects [45, 46].

4.8.3 Operation

In information, system a subject would like to invoke an active process is called operation of access control. This example determines the process of operation in access control. When users enter a card with correct PIN code to ATM machine, here the control program operation is considered a process on the user’s behalf. In addition, numbers of several operations like deposit, balance inquiry and withdrawal are initiated by the subjects [45].

4.8.4 Privileges or Permission

It is that kind of entity of access control to authorize some performance to some action in system. Other hand permission is the term used in access control to combine the operation with object. For example the there is some particular operation in a system done on different two objects which shows two different permission [45].

4.8.5 Access Control List (ACL)

It contains all lists with possible objects in system and mechanism is to specify all subjects where they are able to access the objects in system along with possible initialized rights. In access control list there is a pair of subject with set of rights of each entry. Access Control matrix columns are corresponded to ACL [45].

4.8.6 Access Control Matrix (ACM)

A table of access control where a subject is represented by each row. Each column represents an object. Each new entry in system is included on the set of access rights and initiate usually for that subject to that object. Mostly in Access Control Matrix, subjects do not have the rights for access to objects and called in general sparse. The list of triples in system represents the access control matrix and following is the structure [45].
4.9 Access Control Policy and Model

Usually organization management planning is to implement the approach of access control in system with respect of different abstraction. In system the policies of access control, models concepts and suitable mechanism.

Policy of access control is the requirements of high level to manage the specification of access. How it is possible to manage the access and who will be the responsible to access the information on what kind of circumstances. Applications specific kinds of policies are identified for the access control policies. For example, may consider an applications and different computing platforms. With in health care organization the access control policies may be relevant to competency and privacy.

Through the adequate mechanism in system, the access control policies at high level are obligated and then according to structure of system request of user’s access are translated that usually system provides. Model is described a formal presentation of the system to enforce the security policy.

4.9.1 Discretionary Access Control (DAC)

It is the kind of access control to restrict the access to objects or resources of objects and usually depends on the objects belonging to those resources. Limited amount of access of objects to subjects based on their reasonable relation to appropriate resources.

According to trusted computer system evaluation criteria of department of defense standards (TCSEC), “The TCB shall define and control access between named users’s and named objects (e.g., files and programs) in the ADP system. The enforcement mechanism (e.g., self/group/public controls, access control lists) shall allow users to specify and control sharing of those objects by named individuals, or defined groups of individuals, or by both, and shall provide controls to limit propagation of access rights. The discretionary access control mechanism either shall, by explicit user action or by default, provide that objects are protected from unauthorized access. These access controls shall be capable of including or excluding access to the granularity of a single user. Access permission to an object by users not already possessing access permission shall only be assigned by authorized users” [38].

4.9.2 Mandatory Access Control (MAC)

This kind of access control determines that central body of system is allowable to develop all kind of feasible policies decisions of access and there would be not involvement of individual owner of the object. In addition, the owner in system is not permitted to modify the access rights. Often the MAC policies depend on the labeling mechanism with set of interfaces.

For example, at secret classification level, users in system give a running process with label of secret and forbidden him to read out the nature of file with fixing of label with name top secret. We are able to call this as “simple rule of MAC”. Another example, the users in
system give a running process with label of secret and forbidden him to write in file with fixing of label with name confidential. That kind of rule in system is known as strict star property or “strict * property” [45].

4.9.3 Role Based Access Control (RBAC)

RBAC is the access control where every kind of decision in system depends on the roles. However, the individual users in organization are element of system and they are acquiring according to their assigned role.

“Access rights are grouped by role name and the use of resources is restricted to individuals authorized to assume the associated role” [45].

A good example of hospital system, role of doctor in hospital system is to execute the diagnostic, prescribe the medication and viewing the laboratory test of analyzed disease. Beside researcher has own role to have the anonymous clinical data for the purpose of study. Successful resources of Role Base Access Control (RBAC) mostly in organization system develop and enforce the enterprise specific security policy. In addition to develop the security management process of system for reformation [45].

In a range of RBAC components, embodiment of access control policy is in the following outlook. Just like as Role-permission, user- role and role-role permission. Subject and object are the traditional aspect of access control and some time the users of access control may have number of subjects with respect of different permission at the same time. The main components of RBCA are users, roles, permissions and sessions [47].

4.9.4 Dynamic, Context-Aware Access Control

Current system security architecture of organizations to fulfill the security and privacy requirements of sensitive information of health care is still open question. At present mostly security requirements of organizations solved by RBAC model but still address the problems to security requirements to applications of healthcare [48].

Healthcare has sensitive information of electronic health records and an account of security purpose healthcare requires on demand authentication, extensive context-aware access control and dynamic authorization enforcement to fulfill the security and privacy requirement [48].

The capability of dynamic Role Based Access control (DRBAC) is to generate dynamically decision that based on the context information. The business of DRBAC is to regulate dynamically the Role assignments with permission assignment that based on the context information [49].

- **USERS**: Users are the entity of DRBAC whose all accessibility in system is controlled. Users are the set of users.

- **ROLES**: Roles are the business functions according to context of organization with semantics association regarding of authority in organization. In addition regarding of
responsibility the control of organization assigns the users to role. Roles are the set of roles.

- **PERMS**: The permissions are the authorization and endorsement to access in system for number of sensitive protected resources. A PERM is the set of permissions.

- **ENVS**: set of context information called the ENVS in system. “We use an authorized “Context Agent” to collect context information in our system”.

- **Sessions**: the interaction between the subject and object in system called the set of sessions. At each session set of roles assigns to users and “the active role will be changed dynamically among the assigned roles for each interaction”.

- **UA**: that is mapping approach that users have assigned a role in system. A set of roles assigns to each users in each session in system. Here it is the context information, used in system for decision to know the active role. So resources are accessed with role in system.

- **PA**: it is mapping approach that assigns the permission in system to role. Role with privileges for accessing the resources gives permissions. The context information in system makes decision to know what kind of permission is active for role.

These are the fundamental components used by Dynamic role base access control [49]. The new DRBAC model makes a dynamic decision for authorization with the support of context information. Extensibility and flexibility are good features to fulfill the security requirement of organization. Current Role Base access control is static access control with poor configuration of flexibility and extensibility. This poor configuration of RBAC is replaced by the Dynamic role base access control DRBAC [50].
The figure 8 depicts the architecture for Dynamic Role Base Access control. This infrastructure is consisting three main components i.e. authentication engine, authorization engine and context services [48].

In informational system, the authentication engine is using to issue the biometric authentication token to clients in order to create trust level or authentication level. The authentication engine authenticates the users credential information in system against the database of enrolled identities. The responsibility of authorization engine in system is to investigate the data access when the possible requests are coming from application services. Context service is to extend the RBAC model in system. The function of that model is to maintain all pre define context types and dynamically make evaluation. At the end, generate the results to authorization engine. It is used to manage the context definitions with security
structures repository. The authorization engine in order to encounters the context type needs the context services to make evaluation of the context type [48].

### 4.10 Across Border (Client-Server) Communication

The electronic health records of patients are very important and it is necessary to protect and secure from unauthorized users. The Electronic Health Records (EHR) is communication among different healthcare personnel along with across boarder. To introduce the Virtual Private Network (VPN) technology with introducing of Secure Socket layer (SSL) to make sure the security of sensitive information when they are transferred over network among the users in healthcare for good treatment. Secure Socket layer (SSL) is the layer to provide good security to data integrity when it transferred over the network. Secure Socket layer (SSL) is the protocol to use security purpose when the sensitive information is transformed between the client and server [56].

In addition, the Inter-process communication (IPC) is another approach to use in communication when the data is exchanged from one place to other through network [56].

![Client and Server Communication and interaction](image)

**Figure 10: Client and Server Communication and interaction [56]**

### 4.11 Security Analysis Approach

There are several collections of approaches (tools and techniques) available and used by the different organization regarding security analysis. For example, Information Security Management System (ISMS) usually based on ISO standards, policies and risk management, and assessment.
4.11.1 Information Security Management System (ISMS)

The new systematic approach and management perception of Information security management system (ISMS) base on ISO standards and the purpose of this management is the protection of the sensitive information of any organizations regarding of security and privacy and eliminate the possible loss and failure. Certain environments like different users or stakeholders, information processing structure and information technology are contained to support the ISMS. However, it is pure management system and designed to establish, monitor, implement, operate, maintain and improve the characteristic of information security by the collaboration of different activities, various techniques and tools in organization. While this management system of information security work on two different levels like system level and process level. The system level contains the process of level tasks and it has been included organizational structure, process and resources. Other level is process level concerned to development, implementation, planning, maintenance and evaluation of the IT security [35, 32].

4.11.2 Plan DO Check Act Approach (PDCA)

According to ISO 27001 standards, in organization the function of this PDCA is to establish, planning, operation and maintaining the information security. So in order to attain the goals the whole process is represented by the approach of PDCA [35]. According to figure 11 it has four different steps to perform on repeatedly execution. The first step of (PDCA) has set up the policy of ISMS. According to the requirement and policy of organizations the objectives, procedures and whole process are considered significant to manage the security risk and support to improve the information security. The second step of ISMS policy has the objective of implementation and its operation. The third step of ISMS policy has determined the measurement concern to performance of monitoring and effectiveness of ISMS. The different consequences are brought to management with respect of review. The last step defined the approach of corrective and preventive environment usually based on those above three different steps consequences [35].

![Figure 11: Information security management system (ISMS) [35]](image-url)
4.11.3 ISO Standards of Information Security Management System

International standard organization (ISO) has defined some standards concern to information security. The provider of those standards was BSI management system and intended to provide the information security policy and identify key information assets of organization [33].


Proposed to provide the significant requirement of establishing, implementation, monitoring, maintaining and improving the information security management system. It provides the adequate security control and aim to protect the asset of information as well as ensure the confidence. For the following purpose, that code is used to ensure the appropriate security.

Development of security requirements, ensure the security risks that are typically costly to manage, ensure the law and regulations, appropriate framework for controlling of implementation and management to ensure such security objectives, innovative environment for information security. That kind of security code deals with following characteristic secrecy, accessibility and accuracy of information security. According to involvement of this code the secrecy deals with right authorizer has availability of the information. The accuracy deals with that information that should be protected and it should be accurate and complete. The last term accessibility deal with that user has accessed that information where they have to be required [36, 4].


“A Code of practice for Information Security Management and guidelines in order to control the information security [33]”. It contains control of objectives and having the following areas related to information security management.

Maintain security policy, organizing the information security, management of assets of organization, physical security, management for communication and operations, access control, maintenance and development of information system, management for information security etc [53, 4].

Therefore, the ISO/IEC standards have controlled the objectives purpose and to be determined to find out the requirements initiated by risk assessment. It has to provide the practical guidelines in order to develop security standards for effective management of security system.

4.12 HIPPA Security Standards

There are four different information security standards proposed by the Health Insurance Portability and Accountability Act (HIPPA) under the United States Department of Health and Human Services (DHHS). The successful movement of the HIPPA under DHHS is to develop the standards with those feasible requirements to maintain as well as transmit the electronic health records of patients in health care system. HIPPA standards aim to enhance the efficiency with effectiveness of the health care organizations when the sensitive information is transferred through electronically. Due to the HIPPA standards the confidentiality of information of health care has and protects the security is maintained [40].
Therefore, the HIPPA has applied some security standards to maintain the information of health care secure and keep the confidentiality and privacy of electronic health records. These security standards or rule usually deals with electronic protected health information (EPHI) [40].

a) Administrative procedure
b) Physical safeguard
c) Technical data security services
d) Technical security mechanisms

4.12.1 Administrative Procedure

It is designed to comply with act by the policies and procedures. That kind of administrative procedure is used to maintain the protection of data integrity, data availability and data confidentiality in health care system. Some time it is said a formal procedure to carry out the measures of information security. Some time called personnel procedures [40].

4.12.2 Physical Safeguards

The physical safeguard security standard is to deal with controlling physical access to protect the data against unauthorized access. The physical safeguards is not only used in organization to protect the data integrity, data availability and data confidentiality but also keep protection of physical computer environment system, instruments to be protected from fire and also intrusion. It prefers mostly to use the control access to computer system [40].

4.12.3 Technical data security services

The technical data security service is to deal with controlling access to computer system information and protect the communications when it is transmitted along over several networks electronically. Similarly before it has to protect the data integrity, data confidentiality and availability but the mainly it does have comprise those process which are used for protection, control and monitoring the information access. The risks management as well as risk analysis is important to imply the acts security requirement at minimum level of standards [40].

4.12.4 Technical security mechanisms

Technical security mechanisms are the term used to prevent those who are not authorized to access the data during when the data is being transmitted through network. Simple it performs to protect the data when it has been transmitted through network [40].

4.13 Evaluation Technique

There is number of evaluation techniques available that is considered the base of information security. The risk analysis evaluation technique, risk management, risk assessment and
safety testing technique are the approach to identify the risk and validate the possible threats of risks [37].

4.13.1 Risk Management Evaluation Technique

In recent years it was mostly controversial issues to be acquainted, how the technology environment makes threaten the security, privacy about information of patients, electronic health records and patients e-journals and so on. However, through fast development and improvement of different technology has protected the information of health care system obviously [43].

In organization to classify such level of security the approach of risk analysis is widely used by the expert of information security. The implementation of risk analysis in system is to protect the assets or information of system efficiently and cost-effective when it has been installed. When information security to be planned for any system so it is important prior to consider the identification of existing risks in system. Consequently, the identification of risk is the key concept for this purpose to design and implement apparently the mechanisms of security in system [4]. However to ensure the information security risk assessment appropriately guidelines of information security risk management with risk management standard contribute the common methodology.

Therefore, the whole process to investigate is performed by the risk management as regards to establish context, initiate the identification of vulnerability, threats and having the mechanism for possible analysis, risk control, risk prioritization, implementation, monitoring and maintenance. Probably these are term anticipated by the risk management in organization to protect the assets or information of system.

Similarly, the concept of risk assessment initiates the establishment of context, identification of vulnerability, threats, analysis and risk prioritization.

Therefore the risk management process concern to information security risk assessment and information security management propose the information assets prior, identify also those threats are faced to organization. So after improved performance of information security risk assessment the process of information security risk management apply the successful implementation of effective control mechanism to maintain the cost of control with such level of security. Therefore number of process are involved to fulfill the requirement of risk management standards, for example it has included the following process context establish, risk identification, risk analysis and risk evaluation [4].

According to the book of DOUGLAS written in 1992, he preferred the risk explanation as "Risk refers to external dangers such as natural disasters and threatening behavior by enemies". He has explicitly explained risk in system as external and inside threats to the environment and resources of system to bring some possible variation and modification in size and existing structure [37].

“The possibility of loss resulting from a threat, security incident or event". Further risk is to threat to the information of organization [38]. According to risk management or information security risk management is the procedure, where information of organization is valued, identification of threats and vulnerability, possible monitoring and implementation should be measured effectively to protect the information or assets of organization from those to generate a threaten to information security [14].
4.13.2 Standard Risk Analysis

Risk analysis is the detailed procedure or process to make sure the assessment of risks in system. Along with risk management and evaluation to discriminate explicitly the harmful consequences to organization, vulnerabilities and security threats to important assets of electronic health records of health care system [38]. The standard risk analysis methodology is

1) Identify the asset for reviewing
2) ascertain the threats, risks and issue to the asset,
3) Prioritize the risks like vulnerabilities to asset,
4) Implement the corrective measure, safeguards, tools etc.
5) Monitoring the effectiveness of these tools and attempt to assess the effectiveness [42].

Risk analysis performance should be the analytical process to explain that information which is not considered reliable according to desirable dealings. Undesirable events or risk in system whether from internal or external source should be properly analyzed [38].

4.13.3 Risk Assessment Evaluation Technique

The development of security evaluation mechanism is a procedure used by the organization to achieve the objectives of security in order to continue properly the functionality of all kind of users [27]. That kind of procedure is to measure the assurance of possible identification, management process and controlling the risks to organizations. Having these different measures has to ensure the security objective of organizations for example data or information availability, data integrity, confidentiality and concept of accountability [27].

For that purpose to develop and design those security techniques or mechanisms for the organization to evaluate and monitoring the system information appropriately, that's why the risk analysis and risk assessment has playing significant role in system for the designing of security mechanism. The risk assessment is the procedure used in system to investigate all exterior and interior threats related to security risks to the sensitive information or assets of organization [39]. Some important guidelines are proposed by the ASIS foundation that is following.

- Organization should be realized in detail and assets along with people working in organization must be identified which are at risk.
- Often attempt to discover the vulnerabilities or risk events in system.
- Have the possibility to loss risk and regularity of events.
- The events should be impacted.
- Cost and benefit analysis approach.
4.14 Swedish Healthcare Laws and Regulation

Wide range of provisions of legislative designed for Swedish health care for protection of sensitive information is existing. Following are the some basic acts of constitutional legislative acts to ensure the confidentiality and privacy sensitive information [51].

- **Patient Record Act**

Patient Record Act (SFS 1985:562) is an act designed for Swedish healthcare. The function of this act is to protect the documentation or paper based of sensitive information of patients in Swedish health care. Sensitive health information of patient in Swedish health care recorded on paper based should be secured properly from unauthorized access [51, 11].

- **Secrecy act**

Secrecy acts (SFS 1980:100) is designed for maintaining the professional secrecy at public environment and confine to distribute the public document. Main purpose is to secure the citizen’s privacy. Individuals to expose the sensitive information in their private circumstances cause the disadvantages [51, 11].

- **Personal Data Act**

Personal data Act (SFS 1998:204) is designed for protection of personnel integrity of patients in health care. This act also becomes accustomed to EU rules [51, 11].

- **Healthcare Records Act**

Health Care Records Act (SFS 1998:544) is to protect the care records like care in infection protection, psychiatric compulsion care, dental care, legal psychiatric care. It is designed to protect all kind of care records in health care [51, 11].

There is Number of regulations and laws designed for Swedish healthcare for example Health and Medical Services Act (SFS 1982:763), Medical Care Field Act (SFS 1998:531) [51, 11].

![Image](image.png)

Figure 12: The six Acts that cause an impact on healthcare [51]
CHAPTER 5: EMPIRICAL WORK

In this chapter, we have discussed the empirical work for our thesis. That empirical work explains what techniques/methods are used by the authors for the collection of result as well as. We have conducted several interviews and case study from different healthcare personnel, who are working in Blekinge county health care since many years. Before conducting the interview and case study, the authors have planned to choose the appropriate personnel who have relevant experience and expertise about the management of information security of electronic health records or patient’s information in Blekinge health care. Therefore, we have offered our designed prospective to number of healthcare professional regarding collection of different information.

5.1 Conducting Case Study

The case study was conducted for the collection of relevant information of the current environment about management of information security in Blekinge Healthcare. The main purpose of the case study was evaluation of Healthcare organization based on significant ICT implementation. The existing environment of Blekinge Healthcare has fully adopted the implementation of ICT environment.

The management of Healthcare is able to maintain the information security mechanism through ICT implementation. The Blekinge Health care is spending huge budget for the management of information security environment, which based on ICT implementation but still management has faced difficulties to maintain the ICT based information security system. The objective of the authors had possible investigated the security features of their system during the conducting interview. To differentiate the current management of information security system based on ICT and explore the causes of issues as well as threats against information security. The aim was to collect the views and ideas of the healthcare professional and general environment.

5.2 Planning Approach

Conducting successful interview as well as case study, the proper planning is the important approach to fulfill the requirements of designed prospective. Therefore, we have emphasized on the proper planning, taking guidance support, management and most important thing was the time schedule. Before conducting this interview and case study, we were able to study number of articles, review of literature, informal meeting with healthcare professional and experts. Those have prepared us to conduct the good case study and interview from healthcare professional. In addition, it supported us to design the questions that are conducted from the number of Healthcare personnel. Before suitable planning support prepared us to achieve our findings and results for research questions.
5.3 Detailed Questions

We have designed prior number of questions for conducting of interviews with intention to ask with details from interviewee personnel of Blekinge health care. The questions were designed according to our research area what we would have to expect to achieve the good quality feedback and recommendations from various personnel of Blekinge health care county.

5.4 Questionnaire Design

The relevant questions were designed before for conducting of interview from Healthcare personnel of Blekinge Health care. Regarding literature review, articles, researcher’s ideas and views, the authors have designed the number of questions to be asked during the interview from number of professional of Healthcare. We have designed almost same questions but in some case, we have asked some relevant questions during the interview from them, which were considered important regarding our research area.

Questions were simple and according to our research area. The questions were sent to Health care concerned professional before conducting the interview in order to keep in mind what is the aim and purpose of research area.

5.5 Purpose of Interview

Interview is the procedure used to collect the qualitative information regarding of research approach [54]. We have conducted structure and the semi-structure interviews for the collection of qualitative information from different health care personnel. We have conducted the interview from several personnel to know how they managing the information security of healthcare. Particularly it was essentially about the collection of data about patient privacy and patient secrecy. The purpose of these designed questionnaires is to achieve the feedback from the staff of health care and effectively the impact to propose the possible guidelines for the patient privacy and secrecy regarding Electronic Health Records (EHRs).

5.6 Interview instrument

In our propose study, the authors have conducted three different interviews in a group of peoples. There were included healthcare personnel, technical and computer department peoples, medical staff and management staff. The authors have used different instruments for recording of interview of respondents. The interviews were conducted mostly face to face in a group with them. They have allowed us to record our interview.

We have used our laptops, mobiles, tap records for conducting the interviews but mainly the interviews were recorded through tap records.
5.7 Interview Realization

To achieve the objective, comprehensive questions were the base of the any interviews. Several personnel of health care were interviewed including management staff, Medical staff and IT technical staff. Before conducting the interview, all wide-ranging questions were sent them for observations of the research. Within two week, we have been informed for the conduction of interviews. In whole, we have conducted three different interviews from different health care personnel regarding information security. Five different personnel from Blekinge county healthcare have been conducted for interviews.

Therefore first interview was conducted in-group from healthcare personnel in Blekinge Hospital (Psychiatry Department). Similarly, the second interview was conducted in-group from two different Healthcare personnel in Blekinge Hospital. Finally, we have interviewed IT staff including information security engineer. The whole process of interviews from different actors of health care of Blekinge County was taken place in a month. The interviews were conducted in discussion together with them at different place and time. The interviewers asked their questions from respective interviewed personnel and they have responded us to the best of their abilities and competence. Mainly every single interview was took time less than an hour.

5.6.1 Interview 1

We have conducted first interview with Ingela Thörnstrom and her trained student at Blekinge Hospital Karlskrona Psychiatry Department, she is the head nurse of psychiatric department at Karlskrona west (Avdeluingschef, psykiatriska motfagningen). She has 30 years experience and expertise in her field and well known about the information security in health care. The aim of this interview was to describe, how the actors (Doctors and nurses) of health care would be able to manage the Electronic Health Records (EHR) regarding information security.

According to the respondent information, security based on ICT has a tremendous role in healthcare system. The focus of this interview was mainly, how to manage patient information, Electronic Health Records (EHR), flow of information among stakeholders in organization along with outside. They have also discussed a lot about the information security implementation but still the management attempt to enhance the information security in several years.

The interview was conducted with head of psychiatric department of Blekinge County. In addition, throughout the interview, we had focused mainly on the number of problems face to current management system and different other factors related to information security were discussed.

According to respondent, the accessibility is the main problem to resources because they are using only well known user name with password (PINs) today, which is probably security threats to sensitive information of Health care system. In discussion, we discussed mainly about awareness (IT experience and knowledge) of information security of healthcare personnel, Electronic Health Records transmission (Transportation), government regulations,
laws and constitutions, appropriate system of logging in health care and security of patient information etc. The respondent has identified the risks management and assessment procedure for the protection of sensitive information of Blekinge Healthcare but she explained more or less about the implementation of the risk management and assessment.

5.6.2 Interview 2

Our second interview was conducted with Thomas Pehrsson and Kristina Bergqvist at the Blekinge Hospital Karlskrona. Thomas Pehrsson is the head of management of policy and IT strategy maker in Blekinge county council while Kristina Bergqvist is working as lawyer in Blekinge state. According to respondents, we have discussed the rules, set of laws, policy, standards, guidelines and regulations for management of information security regarding of patient privacy and patient secrecy. We have also discussed about the authorization process, access control, identification and patient privacy and secrecy.

The concept of this interview conducting was to get possible reflections from theoretical work. What is the possible approach of literature work to support us to achieve the goal?

Regarding security of sensitive information in Healthcare, the respondent has explained that number of administration body (levels) is available in Hospital. For instance, the authorized bodies in Hospital have been provided the access facilities are allowed to access to the records of Electronic Health records.

5.6.3 Interview 3

The third interview was conducted from Annelie Varsson at Wämo centre Karlskrona. She is currently working as IT engineer at Blekinge Healthcare since last six years. She has the expertise of information securities regarding Electronic Health Records, patient sensitive information and electronic health journal. She has education background as IT engineer and is working in Blekinge Hospital since last six years. She has also experience more or less dealing with the security threats because working as IT engineer since long time.

Before conducting the interview, details descriptions of our questions were sent to her in order to achieve good quality feedback. The interview with Annelie assumed to know about the technical issues related to network system, storage (database) and physical security. The accessibility and availability of resources and authorization tools, constitutional legislative acts and laws, information security standards, the flow of communication among different health care organization, logging environment, different policies and procedures for information security were discussed during the interview.

According to respondent, there is an importance of information security for management of Healthcare organization in order to prevent sensitive information from unauthorized users access. She also mentioned certain problems of accessibility and availability (access control) because in Hospital, employees are given well-known user name and secret passwords. Mostly users have to choose the passwords depends on to their way of procedures.
Transportation of sensitive information across border is another issue to Healthcare management and currently depends on traditional way of communication like paper base. The personnel has explained about the current risk management procedure that number of particular peoples with specified software are allowed to manage the risk or threats activities against sensitive information like EHR in Healthcare management system.
CHAPTER 6: RESULTS

Since last decade wide-ranging expending of ICTs, different model, techniques and applications of security have been developed for resources evaluations and setting up the security specifications as regards decrease risk and avoid the incidents to system.

According to National Security Telecommunication and Information System Security (NSTISS) “The protection of information systems against unauthorized access to or modification of information, whether in storage, processing or transit, and against the denial of service to authorized users or the provision of service to unauthorized users, including those measures necessary to detect, document, and counter such threats” [55]. The fast development of information technology has generated different kind of electronic health care applications but still it is an open question that whether current system is able to guarantee the security of sensitive information of healthcare [40].

Therefore, findings of interviews with case study and outcome from different personnel in health care were categorized in different part. These different categories are access control procedures (approach of availability and accessibility resources to legitimate users ), Electronic Health Records (EHR) of healthcare, international and national standards, guidelines with laws in Blekinge health care, across border communication of information, patient privacy and secrecy and awareness of knowledge of information security.

Therefore, for findings we have conducted three interviews from five different personnel in Blekinge health care. The first interview was conducted from head of psychiatry department nurse with her coordinated trained person. The second interview was conducted from the head of IT policy maker management of Blekinge county Health care with his law and policy advisor. Finally, the interview was conduct from IT engineer and an aim of this interview was to achieve IT role concern to information security.

6.1 Access Control Procedure (availability and accessibility)

The interviewee perception was that all information is stored in electronic form and put the records in paper-based form when it is required to somebody. The IT engineer has discussed that we print the information and printed paper based information is available to patients when they request. Additionally they have no direct access to electronic health records and electronic journals of patients.

According to all interviewee from management of IT, policy maker, IT engineer and medical staff have identified that users are facilitated limited and restricted access to resources through Role-base access procedure. Mostly users are not allowed to access other resources in system application except having specified task. Top management is responsible to assign the role and access to those actors who are capable to perform the task, but normally the services are prevented from unauthorized access.

According to IT Engineer and head of psychiatry department determined that Electronic Health Records with electronic journals are not accessed to any individuals in healthcare and
in critical situation, it is a big issue to access relevant records of particular patients due to access control system. She mentioned that in psychiatry department of Blekinge Healthcare has relevant information related to psychiatry journals are accessed only. The psychiatry related information would be closed to access to other departments like medicine ward etc. In special cases like emergency, the doctors working in other section make a request to top management to access the relevant information of patients or any resources. That is a big problem that relevant information is not available appropriately to users at right time when he has to require it. Health care has sensitive information and should have to be pursued it 24 hours a day and seven days a week.

Control access in Blekinge Healthcare is a procedure to authorize the users by their user name and chosen password. Interviewees have explained that User name is the actual name of employee in healthcare system while password is generated according to their desire. The users are required to use current password maximum for one month and next month the password should be changed. This approach is continuing up to six month to change the current password sequentially by the end of every month. Then the users are able to select randomly any password from their available passwords in order to continue appropriately again their login system to Healthcare. They explained also that management system of Healthcare has the issue of auto lock mechanism because some time they have to forget the locking the computers to prevent the resources from unauthorized users. Interviewee personnel were agreed to have the log file in system. Further current log file is assessed after a month to acquaint about the users who used the system for what kind of resources in what time. The log file will be not provided to unauthorized users or peoples in health care in any form [PM, IT, MS].

6.2 Electronic Health Records (EHR) of Blekinge Healthcare

According to Blekinge health care, Electronic Health Records (EHR) is important assets of Healthcare. According to IT engineer IBM DB2 database is used since long time currently to store the Electronic Health Records in Blekinge Healthcare. Centralized database for storing Electronic Health Record with back up is used in Blekinge County and located it in several places.

Due to the old system, to access right information to right place in right time with some privileges on application is the issue, when requests are sent to application. So providing the required information it will have to take long time to response back. Only the information of Electronic Health Records is provided to doctor when they make a request otherwise prevent it from accessibility. The problem is depriving the patients from right treatment at right time.

IT engineer has explained that only database administrator is responsible person to retrieve and manage the information in database. When the doctor makes a request then their request is analyzed to make sure, whether he/she should be required the information certainly or not. After confirmation with authentication, the information is accessible to doctor for treatment of the patients. Several functions like deletion, adding, changing etc are allowed in journal to those people, who requests to system administrator. So generally, the problem is that if he does not have a request to system administrators then the issue is delayed treatment of patients.
According to top management of IT policy maker in Blekinge Healthcare, number of regulations, policy and laws are used to protect the sensitive information (EHR) in health care. These kinds of policies are issued for protection of sensitive information by the top management level of Blekinge Healthcare. In addition, the Swedish government also makes laws and regulations for protection of sensitive information for Healthcare organizations. As well, the management of IT policy maker has to make the policies with support of Swedish legislations regarding information security and emphases on protection of Electronic Health Records from unauthorized users’ access. Over all access to resources can be properly controlled and required information are available to those authorized personnel after proper evaluation of authentication and verification process.

The lack of knowledge of proper information security for Electronic Health Records is main issue to causes the security risk to sensitive information. Mostly users have provided well-organized software but still it is not adequately tailored regarding security of Electronic Health Records where it has need [PM, IT, MS].

### 6.3 Law, Standards, guidelines of health care

Different kind of laws, standards and guidelines are available in Blekinge healthcare today. The management of IT policy maker with law advisor has expressed that not many laws and guidelines for protection of Electronic Health Records regarding information security are available. The Swedish constitutional legislative acts have specified laws for protection of sensitive resources of healthcare. The Blekinge health care personnel have the requirements and needs of some standards in future to fulfill the security requirements. Limited and concerned standard were found in Blekinge health care for protection of sensitive information, which were not able to accomplish the security requirements. There were the implementation of such policies and strategies currently developed by the political and strategy maker for the protection of information security but still require needs of attention.

The psychiatry department has explained that the government authority is able to set up standards and laws for protection of sensitive information The management of IT policy makers generates guidelines and these guidelines support the healthcare organization throughout in Sweden. The standards, laws and guidelines are important for all users in Healthcare and available to read out carefully and cautiously. To understand what are possible causes and issues to health care personnel regarding protection of information security in health care. The personals of health care during the employment are not provided the education of laws, standards and constitutions [PM, IT, MS].

### 6.4 Across Border Communication of sensitive information

The sensitive information of patients or electronic health records in health care are communicated some time among Healthcares organizations for high-level treatment. The
Blekinge county health care has to transform Electronic Health Records also to different Healthcare organizations for high-level treatment. It has needed in case of critical situation like emergency. According to IT engineer of Blekinge Healthcare explanations that they have own intranet system in Blekinge Healthcare organizations. They transfer some particular information about Electronic Health Records to other Healthcare organization in Sweden for further treatment investigation but the communication is carried out through traditional way, which is called paper based. In fact, they prefer to send the sensitive information in paper based form to other Health care organizations. That kind of transformation of sensitive information is a security threats to sensitive information patients.

Head of psychiatry department in healthcare has specific data of patients but that data is not possible for users of different departments to access except psychiatry department users. There is centralized database system for storing sensitive information of county citizens’ and it is not compatible to other database system across border.

Interviewee personnel have said that transformation of information is very slow procedure because traditional way of communication across borders. Because the information is sent to other organizations through regular mail, then other organizations will fix to clarify that relevant information are received confidently or not. Other problem is to identify who will be able to receive particular information and who will send the information of patient back for confirmation. The unified system of Electronic Health Record is available only in Blekinge County health care. Outside of Blekinge County, it is impossible to access it in Sweden. They intend to have all kind of availability of information across border in Sweden.

They have needed a great attention mainly to work effectively of availability of health care information across border. The personnel said to have the facility for high-level treatment of patient across border in Sweden and patient journals should be available and accessible anywhere in Sweden in order to provide high quality and faster treatment [PM, IT, MS].

6.5 Awareness of Information Security in Blekinge County

Awareness of information security education in Blekinge health care is problem to users. Blekinge Health care employees have been working since long time. When they were employed in Healthcare, that time in Healthcare basic knowledge regarding information security was not provided them.

During employment only basic information are provided to users about the resources, treatment, laws and regulations but still they there is lack of regular framework of information security in health care, regular training and innovative knowledge of information security. Few of them expressed that some users have to attend information security seminar. Mostly the lack of education regarding information security is problem in system to create security risks to sensitive information of healthcare [PM, IT, MS].
6.6 Privacy & Safety of Patient in Healthcare in Blekinge County

Patient privacy and patient safety concern to confidentiality, accountability, integrity, and availability. Currently Role Base Access Control (RBAC) is the process to ensure the information security. According to personnel of Blekinge Healthcare provider, prevention the sensitive information from unauthorized access, Blekinge health care is using the user name with password. The basic aim of this approach is the authentication of users and authorization of resources. For example, database administration is responsible to make sure the security of sensitive data from unauthorized users. Similarly, IT staffs are responsible to keep secure the network system, proper management of physical security (power, fire, alarm system) in order to secure the system from power break down or network down etc. The interviewees have detailed to audit the whole system for security reason after three month in order reduces the security risk or threats. Only concerned body is allowed by administrations for resources to access.

The IT engineer said that implement that kind of software in system to generate automatically a message when unauthorized user try to access the sensitive records. Only the issue is that when somebody leaves his or her system in critical situation the session cannot be expired automatically which cause the security risk to sensitive information. So the sensitive information can be explored to unauthorized users and effect the security of patients [PM, IT, MS].
CHAPTER 7: ANALYSIS AND DISCUSSION

This chapter presents the overall findings of this research by considering the interviewees' responses with support of different metrics. Following are the considering findings of this research.

- **Access Control Procedure (Availability and Accessibility)**
- **Electronic Health Records (EHR) of Blekinge health care**
- **Laws, Standards, Guidelines in Healthcare**
- **Across Border Communication of sensitive information**
- **Awareness of knowledge of Information Security**
- **Privacy of Patient in Healthcare in Blekinge county**

7.1 **Access Control Procedure (Availability and Accessibility)**

Mostly interviewees have responded that extension of different resources (System devices, programs, information and data) setting in health care is considered security issue and risk and difficult for accessible to users if required at right time.

Mostly interviewees said that users are familiar and well known with their current method of authentication (verification) and authorization to get resources but still they have desired that it should be easy to use, advance, fast and more secure.

Few of them were in favor that their current access control for authentication (verification) and authorization to individuals as well as devices should be automatic and flexible and do not have implementation of the role base access control system. Because timing consuming is too much when users make a request to resources or information. Additionally current job role of individual in system for authorization to specific access control list makes the functionality slow down. Nevertheless, access beyond to perform maximum work expose the Healthcare resources to a loss of Integrity, Availability and Confidentiality.

Mostly interviewees recommended strongly having automatic device for authentication and authorization and access to resources through advanced securable technology.

Number of interviewees elaborated that users or individuals (doctors and nurses) in Blekinge health care want to have more access to resources and appropriate information in order to fulfill right treatment of patients during the environment where they have required. However, due to the access control that is considering a question who is the right person for right resources at right time. If at right time the right resources are available to right place, in
Healthcare high quality performance with sophisticated information security can be possible to achieve.

7.2 Electronic Health Records of Blekinge Healthcare

Majority of interviewees believed that Blekinge health care have sensitive information so there should be high security in order to prevent sensitive information from access of unauthorized users. Few of interviewees said that the old storing database is not enough accessible for right information at right place due to roles, privileges and incompatible to technical features. However, the system used for health care information is old one, and it can be down and crashed any time due to many issues like concurrency, number of many queries, failures, and no proper backup server for continuous services.

Regarding integrity, number of interviewees has discussed that retrieval, deletion, change, update are responsibility of the system administrator but reviewing audit to ensure reliable protection of information is log file which is carried out in month once time. Mostly interviewees have said that there is no possibility of internet because Blekinge Healthcare has own intranet system, some time the transmission (communication) of information inside in health care organization creates internal threats to sensitive information like EHR.

Nevertheless, sometimes leaving the system without log off is considered the main risk to system sensitive information that is called probably the violation of confidentiality. Some interviewees believed that the network breakdown is a security threats when there is communication of information from database to stakeholders that affect the performance, reliability and availability of the information and information could be revealed to unauthorized users.

7.3 Laws, Standards and Policy in Blekinge Healthcare

Majority interviewees of Healthcare elaborated the implementation of Swedish constitutional laws in Blekinge health care for protection of sensitive information, records and much more. The explanation of some personnel in them was the availability of insufficient of guidelines and strategy in Blekinge health care regarding information security as well as hardly any appropriate standards. In addition, affirmably they determined with anticipation to introduce the International standards for information security in Blekinge health care.

Few of them interviewees explained that only the top-level management has the responsibility to develop the policy and procedure to configure and audit the information system against security risk regarding sensitive information. Number of interviewees Blekinge Healthcare personnel said that currently Blekinge Healthcare has the Swedish legislation acts with political level policies for protection of sensitive information like Electronic Health records.

Majority has discussed the issue of international standards for protection of different infrastructure of Healthcare.
7.4 Across Border Communication of Sensitive Information

Mostly interviewee response was traditional way of communication (transportation as paper based) to transfer the patient information through across border organization for high level of treatment but the transformation process is very slow and timing consuming. Along with this the currently internet facility for information communication purpose is not being facilitated by the management of Blekinge health care due to the possible security risk and threats to their system.

The paper based is a traditional way to transfer the sensitive information like EHR across borders. Long time is spent by the patient authentication and verification process among Healthcare during the paper based communication. Therefore, it is not good for patient health if condition is decisive.

According to number of interviewees Healthcare, personnel explanations that they have to be secured communication and fast network system among different Healthcare as either system is centralized or decentralized.

Mostly interviewees have determined that there is decentralized system of Electronic Health Records in Sweden so the threat to information security is that who will be the desired individual to receive the sensitive information of patients when that particular information is sent across border. Other side when they receive the information through either a fix or regular mail (Paper based). However, certain kind of problems is existing to receivers in order to know that the acknowledgement of desired information is sent to sender safely or not.

7.5 Awareness of knowledge of Information Security in Blekinge County

According to all interviewees of Blekinge Healthcare personnel observation, that users or individual had not been provided the basic education about sensitive information regarding information security, when they were employed. Still they have not such kind of framework or agenda to provide basic education of information on regular basis.

Some of them have reflected that simply they have been given the opportunity to attend the information security seminar etc and it is considered fundamental issue to provide the awareness of information security in Healthcare individuals on regular bases in order to reduce the possible potential security threats and risks to sensitive information.

Policies of awareness and regular training support strengthen the policies and procedures of security to analyze easily the potential security threats to sensitive information in health care.

7.6 Privacy & Safety of patient in Blekinge Healthcare

Interviewee personnel of Blekinge Healthcare providers said that it is significant to provide good privacy and safety to patient’s sensitive information as well as Electronic Health Records of Healthcare providers. For high-level treatment, first the patients are identified in Healthcare by considering his/her personnel number with parent name if he is accessed
outside from organization through any media. Inside in Healthcare possible identification resources are checked from patients physically i.e. bank photo Id, driving license and passport. Even employees of Blekinge health care are identified through their user name with suitable password. Besides, they indentified to develop reliable and consistent access control mechanism in order to authenticate the users firstly and authorized the resources after properly.

According to interviewees in Blekinge Healthcare the agreements with their employees during the contract of employment for protection of sensitive information was signed. The purpose of agreement is the protection of sensitive information and adapts to CIA mechanisms, contract of non-disclosure and right authorization process to users in health care system. A small breach in CIA of sensitive information of Healthcare causes the disclosing of sensitive information to unauthorized users, fraud risk is increased, and violation is arising to patient privacy. Therefore high quality treatment at right time to patients can be impossible. Other issue is the improper training regarding information security, lack of education about patient privacy and safety.

Through agreements with employees, nobody is permitted in Blekinge Healthcare to see the electronic journals of patients and electronic health records except concerned body. When patient are identified and enrolled to system, his/her journal will be available for medication to concerned personnel in Blekinge Healthcare. Therefore, the agreements with different employees in Healthcare depend on their different level of jobs and access to resources of system.

7.7 Discussion

This part recommends us for explanation of the findings of theoretical work with case study (interviews) of our research. Essentially information security in healthcare organization was the agenda for authors and discussed.

In our discussion, we have to discuss certain things, which are significantly considering issue or problem in term of information security in Blekinge health care.

7.7.1 Risk Management

Health care deals with sensitive information of patients including electronic journals and Electronic Health Records while quality security management and control quality expect much to manipulate all kind of possible security risk to information security in healthcare providers. It is precautionary method to protect the system management from possible threats [57].

7.7.1.1 Access Control Expected Problems (Authentication & Authorization)

In this discussion when unauthorized users attempt to access the resources of access control list without probable accessibility control (authentication and authorization process) generates information security issues. According to current environment, breaches are
existed in their old (authentication and authorization) mechanism and might be vulnerable, and revealed the whole system to unauthorized access.

**ISSUES**

The mechanism to protect the assets of organization on each level apparently based on the CIA principles [26], so the reason currently in health care organization is weak authorization and authentication mechanisms, which do not, fulfills the standards and requirements of CIA principle. Familiar and well-known users name for access to resources (cause actual personnel names of Blekinge health are in use).

Therefore, the information needs to be guessed is password. However, the password of the health care personnel may be according to their birthday results in birthday paradox, traditional names, and pet’s names etc. In addition, unauthorized users will be able to identify these familiar user names with password of individuals to access the records and creates the vulnerabilities to the sensitive information in health care.

7.7.1.2 **Expected Problem of Data Base**

For high quality of treatment, it is social agreement of health care personnel with patients to provide resources to right access at right place and in right time because health care personnel are working with sensitive data of patients and users. System administrator of database should be able to avoid any kind of small vulnerabilities, inconsistency, and risk to electronic health records or database, and keep the system available 24 hours a day and seven days a week. Cause tiny amount of problem or risk as a security risk even arise the situation of casualty of precious life in health care.

**ISSUES**

CIA principles ensure to have appropriate security of organization [26] therefore the reason why vulnerabilities and security threats is generated to database. There is old database used in system, which is not compatible to technical equipments, and instruments and does not fulfill the need and requirements of standards. Unfamiliar personnel are working with database mechanism and creates obstacle. Insufficient routine maintenance in healthcare to audit the database logs and event logs that there has been no misuse of data. Number of different security applications implementation are using in system. There is no backup to continue services and applications used for Spoofing.

7.7.1.3 **Across Border Communication Expected Problems**

For high quality of care, some time Electronic Health Records (EHR) and patients electronic journals are transformed a cross border. It is impossible for Blekinge healthcare provider to transfer the patient sensitive information of Electronic Health records (EHR) through by electronic means. In Blekinge, healthcare Paper based is the traditional way of transformation of information to other health care. The traditional transformation way is insecure to know, who will receive the sensitive information. Moreover, the existing intranet system is used within organization to transform the appropriate information to right place.
ISSUES

Possible reasons to generate security threats and security risks in system as follow. Existed technical equipments for networking purpose in healthcare are not compatible to standards. Currently to computer networks, malware is the threats and risks. Because portable devices might not guarantee proper compatibility, appropriate management for operating system (OS) updates and Non-technical staff in health care is also another issue. Due to number of clients request to resources keep the server down. In way, anticipate paper base transformations of sensitive information be erased, volatile, shuffle and time consuming. In addition receiving acknowledgement back from destination health care due to decentralized system in Sweden is slow.

7.7.2 Policy and Procedures, Laws and Standards in Blekinge Healthcare

In Blekinge County, only the top management of organization imposes health care information security policy and procedures under Swedish constitutional legislative acts. Management’s policies and procedure aim to guide the decision of users and inform the personnel of their responsibilities of security. In health care unavailable, insufficient, and limited standards, policy, and procedures generates the security risks to sensitive information. All Health care organizations in Sweden are monitored by under Swedish constitutional legislative acts, National board of welfare and ministry of health and social affairs [4].

ISSUES

Basic reason of this is the lack of awareness, non-acceptable policies and procedures in health care system. In addition, the policies of current system might not compatible to the standards of International Standards Organization (ISO) and (HIPPA) [26]. Although, the existing policies, procedures and standards are not adequate for end users but the unfortunately same policies and standards are in practice still. Some time the policies, procedures and standards in health care remains neglected. Again, the main reason here is the non-compatibility of the internal architecture with ISO and Health Insurance Portability and Accountability Act HIPPA standards and with national policies and only compatible to local policies and procedures. Furthermore, some policies in health care used to be very complex and not simply easy to understand.

7.7.3 Unawareness

Security threats can be generated to health care assets due to insufficient knowledge and unawareness of information security fundamentals that results in various potential vulnerabilities to the security of any organization.
ISSUES

Personnel are facing unawareness to regular base knowledge of information security in healthcare. In most cases, they do not have sufficient knowledge about the policies and standards or most likely not properly trained about physical security, access control list and information security in general. There is a lack of mechanism for guidance and basic training to support awareness. This implies that, the awareness of a policy needs to be projected in order to ensure accountability.

7.8 Validity Threats

The validity threats are considered important part of any research work and it improves the accuracy of any the research work by identifying those factors, which affect the result. Wohlin have discussed four different type of validity threats which are external validity, construct validity, internal validity and conclusion validity [59]

7.8.1 External Validity

The external validity approach determines to make sure whether the findings and results can be applied to some other domains or not [59]. We can say that the external validity is something that mentions that either the results of the research work are applicable to some other domains.

Wohlin have determined that the intersection of selection and conduction is considered one of the threats to external validity. External validity threats occur when authors selected the wrong subjects from the population. Selection of wrong or not appropriate subject from a population would definitely lead to a situation where the study results cannot be generalized to other domains.

The authors considered the external validity threats to the results and that is why worked hard to minimize this threat in order to have results that can be generalized to other domains also. Regarding this research study, all interviewees were selected from the relevant domain of the research area. All interviewees had a sufficient background of the research area.

The authors had prior meeting and discussions with the health care authorities and after meetings the interviewees were selected and interviews were conducted. The selection was based on the criteria that interviewees have sufficient knowledge of the research area.

7.8.2 Construct Validity

Validity that shows the relation between the theory and observation is called construct validity. The construct validity deals with the generalization of the experiment results to the main idea behind the conduction of that experiment [59].

Wholin [59] explained the evaluation apprehension as a threat to the construct validity of the research work. It explains the human nature that can affect the study results. e.g. sometimes
humans tends to become very smart and clever when during evaluation while on the other hand some people are afraid when they are evaluated [59]. Moreover, this attitude of humans during their evaluation time is something we called construct validity threat as it has the potential to affect the results of the study.

Authors minimized this threat to validity of the results by prior discussion with the interviewees and when they agreed then the interviews were conducted. In addition, the interviewees permission was asked to record the interviews using audio recorder. It was explained to the interviewees that the interviews data will be only used for this research work and then it will be destroyed. In addition, the authors explained that if they like to quote with their names in the research report or they do not. After all these measures, the authors feel that the threat to construct validity is minimized in the context of this research work.

7.8.3 Internal validity

Wohlin [59] explained there are some certain factors that affect the independent variables involved in the research work and even the researchers, for most of time, is not aware of those factors. Internal validity is something that helps researchers to understand and identify these factors [59].

In most of the research works where humans are involved and the empirical data for the research work is collected from humans then it is quite general phenomenon that human feel strange, uncomfortable and some time tense when their voice or videos are recorded. Humans also prefer privacy and that is why sometimes they might feel a little uncomfortable if they come to know that their data will be in research report with their names. All these and such other discomferts and fears are factors that have a potential threat to the internal validity of the research work.

The authors considered those threats to internal validity and took certain measures to eliminate the potential threat to internal validity. The interviewees were asked if its ok with them to use the audio recorder during the interview. The interviewees were given a brief introduction of the research work before interviews. Both the authors identified themselves to the interviewees by showing their student identities just to make the interviewees comfortable and relax. The authors explained that the research work not aims to judge their level of understanding of the technology but rather the focus is on how the system is maintained i.e. EPR. The authors made sure that the data collected during this research work will only be used for the purpose of this research work and that the data will be destroyed after the research work.

7.8.4 Conclusion validity

Conclusion validity is something that ensures the researchers that their results of the research work are reliable enough to guide the researcher to draw the correct conclusion from the results [59]. There are certain threats to conclusion validity of the research work and the authors made necessary efforts in order to mitigate the effects of the threats to conclusion validity.
Wohlin explain the heterogeneity of the subjects, involved in the research work; also possess a potential threat to the conclusion validity of the research work. Heterogeneity is a situation where the subjects involved in the research work have different level of education background and experiences. The difference between the subjects, involved in the research work, pose a potential threat to the conclusion validity [59].

The authors considered this threat to the conclusion validity and took some prior measure before the selection of the interviewees for the research work. It was confirmed that the interviewees involved in the research work has sufficient level of educational background and understanding of the research area. Prior meeting and discussions with the interviewees Blekinge health care system help authors a lot in selecting the interviewees that had comparatively less difference of research area knowledge. It was confirmed that all the interviewees had relevant knowledge and interest in the research area.
CHAPTER 8: EPILOGUE

8.1 Recommendations

The existing information security structure in healthcare management system addresses some challenges to sensitive information. The planning of management is to identify necessary requirements and needs for improvement of information security in healthcare based upon proper analysis of existing backgrounds. Healthcare management system has different security level for stakeholders because of resources granting. The administrative and technical are two different measures and carrying out different job in health care. The sensitive information of healthcare based on these two different measures. Successful management of Health Care Records (EHR) in system is by considering appropriate functioning of both measures with each other to get on demand productivity.

On demand, efficiency of resources in health care through Information communication Technology (ICT) applications creates security problems to management system. By systematic interaction of the users for the system resources is to target the required task is main issue. The problems are existed mainly to access control to ensure the authentication and authorization of end users in order to maintain the information security of healthcare assets. Electronic Health Records (EHR) and Electronic journals of patients are sensitive information of Healthcare and wide ranging protection of sensitive information is necessary to ensure the patient privacy and patient secrecy. The information security model in theoretical work determines the four characteristic have to ensure the information security of health care in term of different security measures. All possible security problems and threats to sensitive information of health care are eliminated if management system follows the principles of information security. Confidentiality, Integrity and Availability (CIA) are principle of information security to fulfill the requirements and needs of security of organization [26].

The policy, procedures, laws and standards are the primary concern in healthcare to ensure the security of Electronic Health Records (EHR) and maintain the security requirements of patient privacy and patient secrecy in healthcare. The local policy and procedure with constitutional legislative acts are implied on the Blekinge healthcare for protection of sensitive information from unauthorized users but still it is open question of introducing of International Standards Organization (ISO) and Health Insurance Portability and Accountability Act (HIPAA) [40].

Healthcare management deals with sensitive information and it is obligation of top management and policy maker to facilitate the infrastructure properly on security education and on regular bases training. Lack of awareness is itself a potential security threats to sensitive information in health care. Without suitable mechanism of awareness in organization, influence the creativity of performance in healthcare and creates obstacles. The Information Technology (IT) personnel in healthcare have significant responsibility and ensure to have provided high level of training and security education. In addition, the importance of security education to is due to the participation Information Technology (IT) personnel in different IT related projects.
Number of security threats and risks are generated i.e. physical security threats, network systems security threats and technical security problems. It is deficiency of analyzing on regular basis in health care to overcome these kinds of potential security threats to system.

Now following are the guidelines and recommendation proposed for the health care after analyzing different factors in investigated area in term of information security for improvement of Electronic Health Records (EHR) in order to ensure patient privacy and patient secrecy.

According to information security model, administrative security and technical security are the fundamental measures of information security to expect further for improvement.

### 8.1.1 Risk Management and Risk Assessment

Authors have proposed the techniques of the proper Risk management and Risk assessment in system for information security. Successfully all possible security risks with threats in system are analyzed and management will continue hopefully to prevent the sensitive information from potential threats and unauthorized access.

### 8.1.2 Information Security Management System (ISMS)

Sometime the management are facing problem to manage the process of information and possible implementation of resources in order to maintain information security. Therefore, we would have to give the guidelines of ISMS to implement in system in order to manage the whole process of information effectively in system. Further, it would be able to minimize the information security risks. Often it works on PLAN-DO-CHECK-ACT to ensure the confidentiality, integrity and availability.

ISMS usually work with International Standards Organization (ISO). We recommend the ISO standards for healthcare to implement for information security purpose. ISO/IEC 27001:2005 and ISO/IEC 27002:2005 are the standards of family of ISO/IEC 27000. The ISO/IEC 27001 will be able for healthcare assets as management control to examine the information security risk against threats and vulnerabilities. While the ISO/IEC 27002:2005 is to entitle to “Information technology - Security techniques - Code of practice for information security management”.

### 8.1.3 Awareness and Advocacy

In healthcare, it is the big shortcomings of awareness and advocacy, which causes the security risk to sensitive information. The authors thoroughly recommend on regular basis the knowledge and education of information security to users. In addition, proper training of information security is necessary for users in healthcare because they process the sensitive information. The awareness and advocacy is most necessary for healthcare personnel to be aware on prior basis.

### 8.1.4 International Constitutional Legislative Acts

Currently national wise and regional wise legislation about information security is used in healthcare for protection of sensitive information. In addition, the regional as well as county
wise policies and procedure is implemented in healthcare but still it does not fulfill the requirements and needs for protection of sensitive information. Therefore, the authors suggest the new policies of management are necessary to adapt to international legislation of healthcare in order to provide better protection to patients sensitive information and system resources.

8.1.5 Access Control

Current healthcare major problem is access control. Who will be able to authentic and authorized for resources. Therefore, the authors have certain suggestion to implement in current system. One is very important is Biometric access control or Smart card system. These two new techniques are very important to make sure the authentication of users and the authorization of any resources. We recommend one other approach, which is very secure and authentic. It is known Single Session Login. Any time when the users of system would like to utilize the resources, through he will generate once time password for login to resources and that password will be completely avoid for next time.

8.1.6 Dynamic–Context Role Base Access Control (DRBAC)

Currently in healthcare Role Base Access, control is approach for accessing the resources, which is static approach. Because “Access rights are grouped by role name and the use of resources is restricted to individuals authorized to assume the associated role” [45]. The author’s suggestion is Dynamic-context Role Base Access Control (DRBAC) because the capability of DRBAC is to generate dynamically decision that based on the context information.

8.1.7 Logging Management with Error control

In healthcare, the logging is important to negotiate nowadays. Sometime the log is verified for error and takes too much time. Therefore, the authors suggest the proper logging management system with error control in healthcare in order to prevent unauthorized access to system resources. The log management with error control will be beneficial to analyze all possible security incidents, violations of rules and policy, fraudulent activities and problems of operation. Therefore, that process will be a complete log to perform complete audit of system. Every kind of faults with failures could be recovered by the system itself. There should be the implementation such mechanism system in organization for error recovery with redoes log files. Therefore, they must have that kind of mechanism with error control to recover the system from critical state.

8.1.8 Standard Software and Hardware

Both standards of hardware and software are important. i.e. current database is very old and do not fulfill the requirement as possible and it is a big potential threats to information security.
Therefore, we suggest the standards software and hardware, which are compatible to all technical measures in healthcare system. Therefore, the management will never face any kind of security threats to sensitive information and resources will be accessed easily.

8.1.9 Virtual private Network with SSL Framework

For high level of quality patients information can be sent across boarder. The system has a week network system for communication will generate security threats and risk to sensitive information. Not only the security threats are possible across boarder but probably inside there is big threats to sensitive information because all time the information is communication in system among different healthcare actors.

Therefore, the authors recommend thoroughly recommend the virtual private network for strong security in healthcare with SSL framework when the information is sent.

8.1.10 Multiple Wide Area Network

For better security, we recommend that healthcare have a Multiple Wide Area Network in order to maintain the continuity of resources transformation.

In case if one WAN become degrade then it is necessary for healthcare to have another WAN and switch to use it automatically in order to provide the resources.

If in healthcare system has no such kind of multiple WAN then it is risk to sensitive information might be lost if there is obstacles to WAN.

8.2 Conclusions

This chapter concluded our contribution emphasizing on information security of healthcare regarding patient security (patient safety and patient secrecy). The main investigated area is the Electronic Health Record (EHR) with electronic patient journals of Blekinge healthcare to ensure the appropriate security to access the right resources and prevent from unauthorized users to access.

We have designed the following questions.

RQ1: What are the problems in information management in investigated area regarding Information security?

RQ2: How these problems could be solved to improve information security of Healthcare?

The investigate area was searched for possible information security threats and risk to sensitive information. Numbers of measures of healthcare observed for problems according to theoretical work and focused the management of administrative measures with technical. In healthcare, it is requirements and great needs of management to focus on security of
There is great effort today of management that right resources available in right time to right place through secure means.

The big problem to management is the access control to make out that sensitive information of patients or Electronic Health records (EHR) must be accessible and available to appropriate personnel when they require for better treatment. However, not avoid the privacy and security of patient sensitive information besides.

The patients in Sweden as well as abroad are moving to across boarder hospitals in order to achieve good care and treatment. Today across boarder, transportation process is very slow due to the decentralized system in Sweden and particular patient’s information takes too much time to identify his/her particulars. Peoples of Sweden do not appreciate this kind of system today but they desire to have securable unified system for fast medical treatment of patients any were in Sweden.

According to Blekinge healthcare personnel, the lack of International standard organization (ISO) with (HIPPA) standards and insufficient roles and guidelines for security, unawareness are issues to solve in future.

Currently the Blekinge Healthcare focus on the Swedish constitution legislative acts to protect the sensitive information regarding of patient privacy and secrecy but it should be developed more with international standards. Information Security Management System (ISMS) based on the International Standards Organizations (ISO) is the needs and requirements for protection of sensitive information from unauthorized user’s access. We have initiated the Dynamic-context Role Base Access Control (DRBAC) with biometric authentication for users and allocation of their resources. Before granting of resources, the users will be identified through biometric authentication process or smart card then the accessibility and availability of respective resources would be granted. The sensitive information will be available 24 hours a day and 7 days week if adopt the compatible database with to introduce the Virtual Private Network (VPN) technology with Secure Sockets Layer SSL framework.

**8.3 Future work**

This research has suggested sufficiently solving the existed problems of information security to management of healthcare system but still it is necessary to find out furthermore the transformation (transportation) of information among different health care organizations in order to enhance more the security of Electronic Health Records (EHR) or patients information. Therefore for investigation thoroughly to conduct more interviews and appropriate case study from different healthcare providers in different counties. The aim of this would be to achieve their opinion and observation regarding Electronic Health Records (EHR) information communications.

Through across border the accessibility and availability of sensitive information of Healthcare organizations is considered open question and needs more concentration to make sure the reliable and trustworthy transportation of Electronic Health Records (EHR) among different counties in Sweden. However Sweden have still to be facing the decentralized Healthcare system and it is being investigated to find out the reliable way in order to provide centralized healthcare system in Sweden.
REFERENCES


PM (policy maker). Head of IT Policy Maker Blekinge Healthcare with Law advisor from Blekinge county Sweden.

IT (information technology). Information technology engineer Blekinge healthcare from Blekinge county Sweden.

MS (Medical staff) Head nurse with trained nurse from psychiatry department Blekinge Healthcare Sweden.
APPENDIX

The following questions asked from medical staff of Blekinge health care organization [61].

1. What is your name and your job description?
   “My name is Ingela Thörnström. I am a head nurse in this department (psychiatry department). I do work with patients but mostly administration. I am also the head of general system here”.

2. How long you have been working in Blekinge health care.
   “I have been working with different things probably of 30 years in Blekinge County. I work always in psychiatric department. Before started worked in healthcare I work in Ericson.”

3. What is identification of patient, when some medication is given to the patient in hospital? Do you have any policies for patient identification?
   “When the patients inter in hospital. Who you are. You know their name, you know their born and nationality before giving prescription. We do not give so much pharmaceutical here. We need patient social security number. We put social security number in the system and all the information are come out in the system. The policies for identification are related to management of policy maker.”

4. If yes then what kind of identity is checked for identification of patient?
   “When you are new patient you should to show identification. Such as driving license, Bank photo ID card and passport. If you are asylum seeker, you should to show LMA card. This card has special number because they don’t have social security number of Sweden.”

5. What kind of agreement was signed with you? What ethical and professional obligations on medical professionals that bounds them to ensure information security?
   “Yes I have to sign to special papers (agreement) that I am not allowed to talk anything about my professional outside. You are not allowed to look at patient journal, which are not related to you. Only the relevant actors are allowed to look at patient journal, which are related to them. This agreement has these all-ethical and professional obligations. The agreement has all these instruction. This contract is necessary for every employee for employment in healthcare”.

6. What are rules and laws of information security concerning to? What do you think that it does fulfill the requirements in organization?
   “It is the same for whole country Sweden and these rules are issue by top management authorities and constitutions legislative. These are only for protection the sensitive information of electronic health records”

7. Do your contracts fulfill the requirement of information security?
   “When I sign the agreement I am never allowed to talk outside. In some special cases, we give the information such as when children are bitten. This is my obligation to give information to community or to police about these children. This
is due to law that healthcare organization will give information to these special authorities.”

8. What are controlling access to sensitive information in health care? (For identification and authentication).
“In psychiatric ward only the psychiatric concern information are access. Only psychiatric journal are access. However, in medicine ward, in common health care they can watch each other in hospital but psychiatric journal are close. During a special cases in hospital, when doctors (healthcare professionals) related with others wards want access to psychiatric journal they request to me and I allowed access to them for the patient which they want access. We have the job role access to users”

9. What is the access control method of information?
“Healthcare organization have special group of people (policy makers) that give access to information. They built policy and then sent this policy to IT section and they implement the policy in the system. For example, in psychiatric I am the head of this and I make the policy for employee that what to do and what not to do and then send this to employee. Employee sign and then I sent this to IT section they put in the system. Some special head doctors have access to most of the data of patient because their job role in healthcare organization.”

10. How patients access their records?
“Healthcare information is only available in healthcare organization. If the patient wants their journal we print on paper, they have no access to hospital journal. Only information is available on computer system, which is directly link to hospital network. The journal are can’t provided online.”

11. How Electronic Health Records are prevented from the access of unauthorized users.
“You have the user name and special code (password). This code is 6 numbers. You should to change this every month. This is six layers which are working in circle, everyone should be used their own code (password). If three times wrong code are used the account is blocked. Then special person will open the account, here I am responsible for this, if someone give wrong code three times the account are blocked. Then they contact me. I check their identity and then open the account with special code.
First, the computer unlocks with username and code then journal unlock through personal user name and code. Usually the user name is same but code is different because the computer code is change every three months but personal user code is change after every month.”

12. Do you have any strategy to improve the protection of information security from unauthorized access?
“The Blekinge healthcare planning to implement the card system with user name and code, it will improve the security.”

13. What should you do, when you leave the computer room?
“When you leave the computer room you should to lock it. If you can’t lock the computer you should to lock the journal. You only press F9 and the computer becomes lock.”

14. Does computer lock automatically when leave it?
“No, it is main problem. When leave their computer room they press F9 to lock the computer. If they cannot lock the computer, they lock patient journal. The computer
system cannot logout after a specific time. Some time the user forgets the logout of the system.”

15. What kind equipments are used in health care system in order to make sure the encryption of information when the information transfers among healthcare organizations?
   “The information is usually are sent through regular mail (paper based), or through Fax, there is no special method for encryption of information because there are no need for encryption in such like close system”.

16. What kind of encryption method is using in health care use? If no so how they are using the procedure to make sure the confidentiality information.
   “The information does not provide through internet (online) therefore there is no need for encryption. The exchange of information about patient is occurring through by mail not by email. If the information is sent to other region (county) of country, the other region (county) will mail to Blekinge county healthcare. Special person of the ward will check the mail identification and authentication. Then this special person sends the relevant patient data through by mail. They will receive there in their own region from post office by showing identification and authentication. In emergency cases, the data is sent through by Fax. When the receiver receives fax, they call to sender to tally the patient name and personal number to identify the right patient record. For security purpose special fax numbers are using for this purpose”.

17. Do you have proper log files mechanism to protect the sensitive information and continue audit the system against security and risks.
   “There is a log file in every system of Blekinge healthcare and by the end of every month the log files are checked against the security threats and risks.

18. Is your organization using any kind of software for the registration of Electronic Health Records of patients?
   “Everything is in the same system and the system is close system”.

19. How the data is stored, is there any centralized or decentralized data base system?
   “Every county council has their own centralized data base system. For example, the Blekinge County has their own, Uppsala and other county their own centralized database system. They cannot access online one another so in Sweden has decentralized system for electronic health records.

20. What do you have to ensure security of Electronic Health Record?
   “In system the concern people who provide the healthcare information are allowed to the specific information of Electronic Health Record. The information will be checked by log files”.

21. Do you have any problem regarding information security of Electronic Health Record?
   “Our system is close system therefore we can’t face so many problems regarding patient information security as well as Electronic Health Record. Other hand I think there is good integrity of patient record because only the concern healthcare person can access the patient record. The extension of the resources in system casues the security risk to sensitive information of health care”.

76
The following questions asked from the top level of management (administrator) of Blekinge health care organization [59].

1. What is your name and your job description?
   “My name is Tomas person and I work as IT strategy manager at the county council of Blekinge.” Me is Kristina Bergqvist

2. How long you have been working in Blekinge health care or outside.
   “I work in Blekinge healthcare almost 30 years and I also work another jobs here related to IT. In 1977, I was the person to introduce information technology (IT) here in Blekinge county council. I also do other jobs before.” (Me Kristina Bergqvist and working here since six months.

3. Have you been received an education of information security in health care system? If yes, what kind of it is?
   “I can’t receive any special education at the time when I was employed because the IT introduced later in healthcare. However, during the job I installed a lot of IT system. Therefore, ultimately you should to know about special knowledge to implement the IT system and about security. But I can’t learn these things from special school, I learn from seminar and from short duration training.”

4. When you gave a job in healthcare, how your identity was verified. Now how the user’s identification is verified?
   “My work in healthcare was that, what kind of IT system healthcare needs and requires, buy and implement them but I was not a professional user therefore I can’t use the system. I help the clinical people that they get the right system. My work is more like a project leader. So now days for identification of person. First, that who are you. The Human resource (HR) department installs all the information about the employs. In addition, the employs are confirmed from system. Identity card is for identification about job services. At system level username is used for identification and password is using for authentication. The password is change after every month. It is just like a cycle.”

5. Doest current authentication ensures the security.
   “The user name with password is not sufficient to ensure the security; we have to implement a new system like smartcards within few years for better authentication and authorization.”

6. What kind of identity of patients is checked?
   “The driving license card, passport or bank photo ID card is used for patient identification.”

7. What are the methods, do you have to ensure security of Electronic Health Records?
   “Only concerned healthcare professionals (employ) in healthcare organization are allowed to check and see the relevant Electronic Health Records, which are concern with him or her” no other body.”

8. What is the access control method?
   “The access control bases on role in organization. They system allowed the services and information which are according to his role. Block the services or
information, which are not related. The head of the department assign the role to employ and the system administrator put the role in the system.”

9. What are organizational policies to secure Electronic Health Records?
   “There are a lot of rules regulations and laws that upper management authorities issued and other special authorities which monitor these in healthcare organization.”

10. Do you have any international laws or police for protection sensitive information?
    “Current we have Swedish government laws and policies but in future it is expected to implement.”

11. What kind of international standards do you have in your organization for information security?
    “The Blekinge healthcare has not yet the international standards but in future ISO standards for information security can be used.”

12. The administration and technical are the security bodies of information security in healthcare, how they solve the risks, risks assessment, and problems concerning to information security.

    “We have not any risk to sensitive information because only concern healthcare providers have accessed to patient records according to his or her role.”

13. What are controlling access methods in system? (For identification and authentication)
    “The patient sensitive information is control according to the organization management authority (Policy makers) rules, regulation and laws and according to the Sweden country base regulation, laws. The IT department of the healthcare implemented these rules and regulations in the system. Some special software are also using for this purpose.”

14. What are strategies and information security policies to secure the sensitive information?
    “Yes, we have policy and strategies from political authorities for sensitive information and communication technology. The healthcare employees must follow these polices.”

15. Questions 40 the existed policies and strategies protect the sensitive information.
    “These are Swedish laws and top management strategies and probably to protect the sensitive information from unauthorized access.”

16. What are the problems of information security to Electronic Health Records Blekinge County, when the information is communicated among stakeholders in healthcare?
    “Every county council has their own healthcare information. The exchange of electronic patient data was not allowed through email but from since July, last year it is possible. Because now the healthcare organizations have, their own trusted secure network system they exchange data through this network. Only concern healthcare professional have approach to this system and access the patient data. Some time when to implement number of such things like programs, physical resources etc”

17. How the sensitive information transformed across borders?
“The traditional way of communication is used like the paper based is the transformation method for sensitive information across borders. It is more time consuming and not properly secure way”

18. What are needs and requirement for Electronic Health records security when it is communicated among users of health care?
   “Blekinge county healthcares are connected through Ethernet. The system is close system only healthcare professional have access to patient data. Therefore, it is secure. Therefore no such requirements are still for security but it is better to implement fast system.”

19. What kind access profile level is used by the current health care system for information security to maintain the integrity, confidentiality and availability?
   “I don’t know properly.”

20. Do you have any strategy to improve the protection of information from unauthorized access?
   “We have new ways of sharing healthcare information and for IT security. However, here in Sweden I cannot listen that any single patient record are hacked. But policy maker try to introduce new things for protection. There should be an advanced technology for authentication and authorization like biometric access control or smart card”

21. When data are sending to other organization, do you encrypt the data?
   “It is forbidden today to send medical record by email or through internet. We have no system for encryption and decryption of data when it is exchange by our special methods. But the databases are encrypted.”

22. Is there any guideline of management to improve security of healthcare record?
   “We have a lot of guidelines, new legislation and rules are coming and we implement them. We also have one person which is the chief of information security.”

The following questions asked from the management IT engineering of Blekinge health care organization [60].

1. How long you have been working in Blekinge health care or outside of Blekinge for this particular job.
   “Since seven years I work in IT department in Blekinge hospital as IT engineer.”

2. Have you been received any special education about information security in health care system? If yes, what kind of education about information security?
   “I don’t have any special education about information security in healthcare because there is no such kind of system to give the information security education.”

Network security

3. Are there any security risks in your healthcare network system also physically security threats?
   “Probably there may security risks in healthcare but I don’t know exactly to identify.”

4. If yes, what kinds of security risks are?
“We have mostly the security risk in our applications that we are using currently in healthcare system because our system is very old. So here we are using old applications for services.”

5. Is the transformation of information in organization among different stakeholder encrypted or across border?
   “The data is sent through wireless to users it is encrypted. It is not encrypted in regular network. Because our system is close system its services is only available in healthcare organizations but we have not the internet use for communication a cross border therefore the paper based method is used for communication.”

6. Do you have possible security for existing networking system?
   “I don’t have so much information about networking but if we secure the applications because here we have old systems which are not secure so much probably.”

Databases

7. How the sensitive information is stored. Do you have distributed database or client server database?
   “Probably I don’t know but we have centralized database and we have a backup of this database in different location.”

8. What kind of database is used in health care system currently?
   “We are using IBM-DB2 databases; this is very old system that we used from last 10 years. At that time system was small but now the system is big it is a problem.”

9. What are risks in database?
   “We have no problem concerning to databases but it is old so.”

Confidentiality

10. What kinds of tools are used for authorization in health care? Further, any improvement do you have.
    “Now days the password with user name is using for authorization purpose in healthcare to access the resources. We are trying to implement the smartcard here. The project is in progress now days.”

11. What do you think about session login implementation in future?
    “This will good for security purpose but create difficulties for medical staff because most of the time they don’t have time. We should to implement such like system which is easy to use”.

12. What are controlling access methods to sensitive information?
    “Every user in healthcare organization has their own login. User name and password. Only this method is used for access controlling purpose. But in future the new technology for authentication is necessary like smart card.”

13. Do you have any strategies with policies to secure Electronic Health Record?
    “I don’t know about this but probably we have to secure the HER.”

14. Do you have any standards for protection of information security?
    “I don’t know about standard which are using here”.

80
15. How the Electronic Health Records is prevented from unauthorized users access.
   “Every user has their own login. This is an issue some time the medical staff leaves
   their computer without lock because they forget. The system session can’t expire
   after a specific time. The user should manually lock the system by pressing F9 to
   lock the computers. It will better if we implement the smart card, which has the
   facility, when the user takes their card the system becomes lock. When the leave
   their system rooms.”

16. Is there any mechanism for session logout after a specified time? Is there any log
   approach implemented to audit the system for security threats, errors, issues etc?
   “The system can’t logout after a specific time. It is manually logout through
   pressing F9. When the F9 is press the system become logout. Now days we are using
   user name and password for login, but now days a project is going which implement
   smart card in future for user login”. Some time the healthcare employees leave there
   computers without logout because most of the time they are busy. They forget their
   computers without lock.”
   “We have also log file approach for security threats, it is investigated by the end of
   every month.”

17. Are there any methods, do you have to ensure security of Electronic Health Records
    with employees and patients records?
   “In system there is separate software when someone looks at your record illegally it
   giving alarming message. No one is allowed to see the patient record except those
   healthcares professional who are concerned with him or her. You should not discuss
   anything of patient records with employs outside”.

18. How you make sure that Electronic Health Records are Confidential here.
   “Yes it is confidential. Only doctors are allowed to that area of patients’ record
   which is necessary for them at time of treatment but some time when needs it in right
   time, it creates problems because access controlling, only specified person is
   allowed to have concern information.”

19. Do you have any plan to improve the protection of information from unauthorized
    access?
   “I don’t know about this. May the management for strategy makers have the
   responsibilities to improve the protection of information.”

**Integrity**

20. How your organizations manage the integrity of Electronic Health Records?
   “There is database administrator in here that is responsible for managing database
   integrity. When someone makes changing in the data, the old data are located in
   database but the system cannot show farther. It also keeps the record that, which
   makes the change in the record. Some area is possible to change and the database
   doesn’t keep record of change data, but it keeps record about sensitive data”.

21. What are security risks to Electronic Health Records of your health care?
   “Some time IT department close the system for maintenance that time only the
   information are readable but changing are not possible. When the system become
down, then they use paper based methods for notation of prescription.”

22. How management is be able to solve security risks in system.
   “I don’t know exactly but sometime if we keep extra network for this, if one close
down the other one take responsibility”.

23. How the information is prevented from unauthorized access in term of integrity.
“Every computer system and user has password and username, most of the time the user name are same but password is change. When authorized user makes changing in data, such as delete, insert etc the database keeps the history of changed data. However, it cannot show the changed data to user. But system administrator has responsibility. It also show that who delete the data and about the time that change are made.”

**Risk management**

24. How risk management is managing in system?
   “We have group of people which take care of this, and also special software for this. We have virus protection, firewall. Everything is narrow down and has proper logs to audit the security threats.”

25. Does the existed risk management solve threats and risks properly?
   “I don’t know about this may be”.

26. What are networks and systems security risks in system in Blekinge health care?
   “I don’t know about this topic what are the security risk and how they are managed.”