NETWORK SECURITY VULNERABILITIES AND PERSONAL PRIVACY ISSUES IN HEALTHCARE INFORMATION SYSTEMS: A CASE STUDY IN A PRIVATE HOSPITAL

by

Nihan Namoğlu Cengiz

B.S., in Electrical Engineering, Yıldız Technical University, 2005

Submitted to the Institute of Biomedical Engineering
in partial fulfillment of the requirements
for the degree of
Master of Science
in
Biomedical Engineering

Boğaziçi University
2014

NETWORK SECURITY VULNERABILITIES AND PERSONAL PRIVACY ISSUES IN HEALTHCARE INFORMATION SYSTEMS: A CASE STUDY IN A PRIVATE HOSPITAL

APPROVED BY:

Prof. Dr. Yekta Ülgen (Thesis Advisor)	....
Prof. Dr. Albert Güveniş	....
Asst. Prof. Dr. Selçuk Baktır	....

DATE OF APPROVAL: 19 June 2014

ACKNOWLEDGMENTS

I would like to thank my supervisor, Prof. Dr. Yekta Ülgen, for his guidance and patience throughout my graduate studies. He has always motivated me throughout this study.

I want to express my special thanks to Ahmet Atasoy who has been extremely helpful even with the issues that he is not too much familiar with. I believe he will always be a great researcher and an academician that one would like to work with.

I am excessively grateful to the Institute of Biomedical Engineering for allowing me make great friends and creating the fortune of meeting my dear friend Eda Çapa. She has spent many evenings and weekends studying with me at the Institute as those were my only available time due to my work load. I deeply wish all the success that she desires.

I would also like to thank my professors, Prof. Dr. Halit Pastacı and Prof. Dr. Galip Cansever, from Yıldız Technical University for their encouragement to route my way to biomedical field during my undergraduate education.

Finally, I would also like to add my gratitude for my family. I would like to thank my parents and my sister for their helping hands and all the support they provided me throughout all my education. I would, finally, like to thank my husband, Harun Cengiz, for his presence in my life and really appreciate his patience and support.

ABSTRACT

NETWORK SECURITY VULNERABILITIES AND PERSONAL PRIVACY ISSUES IN HEALTHCARE INFORMATION SYSTEMS: A CASE STUDY IN A PRIVATE HOSPITAL

Healthcare industry has become widely dependent on information technology and internet; as it moves from paper to electronic records. Despite the benefits of electronic system, good quality may not be totally achieved unless its risks to security are mitigated. Working in collaboration with a 150 bed private hospital in Turkey; this study aims to present a secure healthcare network infrastructure while presenting the security vulnerabilities in the current hospital information systems. The regulation criteria in Turkey and counterparts in USA and EU are compared according to their privacy approach and a list of items for common security controls from different industries is proposed as a best practice. The study shows that the hospital is not compliant with known healthcare standards like HIPAA or ISO 80001. Managements attitude against privacy and security shows that the responsibility is totally to IT and Biomedical Engineering Departments. Since explaining the threats and corresponding vulnerabilities in the system may cause the hospital be prone to cyber-attacks, the name of the hospital is secluded. As hospitals are adopting electronic transactions, consideration must be given to protect public electronic health records in terms of personal privacy aspects. Healthcare industry in Turkey should benefit from best practices in other industries and applications in other countries. This study can lead the pathway for policy makers in healthcare organizations and regulation authorities to implement a more secure environment for every citizen.

Keywords: Security, Privacy, Electronic Health Records, Personal Health Records, EHR, PHR, Cyber Threats, Hospital Information System, HIPAA, ISO80001, ISO27001, Healthcare Regulations.

ÖZET

SAĞLIK BİLGİ SİSTEMLERİNDE AĞ GÜVENLİĞİ ZAAFİYETLERİ VE KİŞİSEL MAHREMİYET SORUNLARI: ÖZEL BİR HASTANEDE VAKA ANALİZİ

Sağlık sektörü, kağıt belgelerden elektronik kayıtlara geçişle birlikte, bilgi teknolojileri ve internete oldukça bağımlı hale gelmiştir. Elektronik kayıtların maruz kalabileceği güvenlik risklerine karşı tedbirler alınmadığı sürece kaliteli bir sistem elde etmek mümkün olmayacaktır. Bu çalışmada, Türkiyede özel bir hastane ile ortak çalışılmış ve hastane bilgi sistemlerindeki güvenlik zaafiyetleri ortaya koyularak hastane sistemleri için güvenli bir ağ altyapısının önerilmesi hedeflenmiştir. Türkiyedeki düzenlemelere ait kriterler ABD ve ABdeki kriterler ile karşılaştırılmış; farklı sektörlerin uyguladığı ve sağlık sektöründe de uygulanabilecek iyi uygulamaları içeren güvenlik kontrolleri sunulmuştur. Çalışma, hastanenin HIPAA ve ISO 80001 gibi bilinen sağlık standartlarına uyumlu olmadığını göstermektedir. Hastane yönetiminin kişisel mahremiyet ve güvenlik konularına yaklaşımının destekleyici olmadığı ve sorumluluğun IT ve Biyomedikal Mühendisliği Departmanlarına bırakıldığı görülmektedir. Tehditler ve mevcut sistemdeki zaafiyetler sıralanırken hastanenin ileride siber tehditlere karşı mağdur olmaması açısından, hastanenin adı açıklanmamıştır. Hastanelerin elektronik ortama geçişiyle birlikte, vatandaşların elektronik sağlık kayıtlarının korunması, kişisel mahremiyeti sağlamak açısından zorunlu hale getirilmelidir. Bu çalışma sağlık sektöründe politikaları belirleyenlere ve düzenleyici otoritelere vatandaşlar için güvenli bir ortam oluşturma konusunda yol gösterici olabilir.

Anahtar Sözcükler: Güvenlik, Mahremiyet, Elektonik Sağlık Kaydı, Kişisel Sağlık Kaydı, Kişisel Veri, Siber Tehdit, Hastane Bilişim Sistemi, HIPAA, ISO80001, ISO27001, Bilgi Güvenliği, Ağ Güvenliği, Sağlık Mevzatı, Sağlık Regülasyonları.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF ABBREVIATIONS

AAMI	Association for the Advancement of Medical Instrumentation
ANSI	American National Standards Institute
AV	Antivirus
COBIT	Control Objectives for Information and Related Technology
DB	Database
DDOS	Distributed Denial of Service
DLP	Data Leakage Prevention / Data Loss Prevention
DOS	Denial of Service
EHR	Electronic Health Records
FTP	File Transfer Protocol
HA	High Availability
HIPAA	Health Insurance Portability and Accountability Act
HIS	Hospital Information Systems
HQS	Hospital Quality Standard
IEC	International Electrotechnical Commission
IETF	Internet Engineering Task Force
IPS	Intrusion Prevention System
ISO	Internation Standards Organization
IT	Information Technology
LAN	Local Area Network
LDAP	Leightweight Directory Access Protocol
NSA	National Security Agency
NSI	National Security Institute
P2P	Point to point
PACS	Picture Archiving and Communication System
PHI	Personal Health Information
PHR	Personal Health Records

1. INTRODUCTION

In today's modern world, it is crucial to record and document, every patient's medical history and health services provided including his recovery progress. The hospital databases are of great importance of personal payment data, social security numbers, private insurance numbers, electronic health records, radiological images and hospital's own financial data. With the increase in the number of mobile devices and medical devices that support wireless or wireline adaptors to connect to internet, the number of client machines that connect to the critical databases increases; which in turn increases the security risks for uncontrolled machines and intensive data flow. Many hospitals across the world have been and are still being negatively affected by cyber-attacks and data theft [2]. Results are dramatic since valuable and mission critical information is being stolen and the harm given by these cyber threats are irreversible. Hospitals cannot afford any outages or loss of communication caused by denial of service (DOS) attacks. This requirement causes some processes to be redefined according to technological changes, which in turn causes healthcare to be dependent of technology and IT.

Especially with the increase of web applications since year 2000s, hospitals got its own share from cyber threats similarly to other industries in the world. In the USA. the government took a step forward to protect patient records and to impose penalties on hospitals who do not protect sensitive information. The healthcare IT standard in USA, HIPAA, is short for Health Insurance Portability and Accountability Act and covers management of electronic records and the routine procedures for storage systems, backups, software upgrades, access and authorization issues and, most importantly, the security of data being stored.

According to the current practices, the the most commonly accreditation used in private hospitals in Turkey is JCI, Joint Commission International. JCI audits hospitals according to electrical and physical safety that may be introduced on patients.

However, it lacks general IT audits, security of patient records by means of both medical, personal and credit card or payment information and safety of hospital's own financial data. With the integration of hospital and pharmacy records with Social Security Institute, known as SGK in Turkey, personal security issues became the main topic across public opinion and media. The E-health project currently being driven by Ministry of Health is still under discussion with the questions if data transaction will be secure between corporates; and if access to personal records will be limited to authorized personnel. The current network and security technology has the possibilities to control and check this kind of secure data storage, secure data tunneling between corporates, access and authorization rights.

Health Information Systems and Decision Support Systems can be improved as technology evolves. However, it is not always that easy to change and improve processes even if this is for the patient's own good. Although, the ICT (Information and Communication Technology) world allows, it is usually possible to apply these technological changes to the common systems only with obligation and the necessity of standards, laws and regulations.

This study aims to present the vulnerabilities in the current systems and the necessity that can be added to the audit procedures for privacy and standardization. Therefore, we have conducted a case study with the IT department of a 150-bed private hospital in Istanbul, Turkey. (Due to the confidentiality agreement held between the IT Department of the hospital and us, the name of the hospital is secluded for security reasons.) In this study, we have focused on the security of the data stored and transmitted between patients, hospital staff and other corporates while ensuring patient centric privacy.

2. INFORMATION SECURITY AND PERSONAL PRIVACY IN HEALTHCARE

Privacy in healthcare is an underlying principle that focuses on patients and the information that they share with their clinicians and insurance institutions [2]. Patient information is collected when he/she gets an appointment, visits the hospital for a treatment, goes for a diagnosis and makes payment or shares personal insurance and contact information. The amount of information gathered increases each day as patient history is collected on each visit to different health departments, laboratory results and large-sized digital image files [3]. As healthcare industry moves from paper to electronic records, the size of collected data increases and the issue of managing the data securely gets more complex. Patient health information (PHI) is encouraged to be stored in electronic systems, called Hospital Information Systems (HIS) in Turkey. Using HIS across healthcare organizations reduces medical errors, increases service quality and reduces costs. HIS has the following modules:

- Patient admission
- Patient appointment
- Clinical module
- Inpatient
- Outpatient
- Payment
- Laboratory
- Pathology
- Radiology (RIS)
- Surgery Module

- Medical Device Inventory
- Stock Tracking and Purchasing
- Drug Store and pharmacy
- Personnel Module
- Statistics and Reports

Although all the information stored in these modules are important, the information that we deal in this study is the information known as "Protected Health Record (PHR)" or "Electronic Health Record(EHR)". That means anything collected from the patient. PHI or EHR can compromise of:

- Patient personal and contact information
- Patient journal/history
- Pathology Results
- Appointment schedules
- Patient medication
- Laboratory Results

All these data are important. They are stored in different databases and should be carefully kept in secure places. Then comes the problem of managing and protecting many different databases and applications. Ministry of Health is driving the E-health project that is interconnecting all hospital and pharmacy networks across the country and creating a central database. It is still a question

- if data transaction will be secure between corporates and
- if really and only authorized personnel will have the right to reach the records.

The security concerns arise because many healthcare applications are web based. According to Worldwide Infrastructure Security Report in 2010 announced by Arbor Networks[1] , web applications and HTTP are the top targets for cyber threats. If a hospital network is hacked by cyber criminals, loss of availability and service would be unacceptable and the attack could also cause financial losses and prestige for the healthcare itself. Most importantly, loss of life is even possible if mission-critical applications and systems are brought down by a DDOS attack for hours or even days. Average outage resulting from a DDOS attack is between 2 - 6 hours and some attacks can run for multiple days or weeks[1]. Any of the following organizations can be a target for a DDOS attack:

- State or private hospitals
- Pharmaceutical firms
- Medical Groups
- Ministry of Health
- Social Security Institute (e.g. known as SGK in Turkey)
- Private health insurance

The attack motivations for the hackers or hacker groups can be:

- Disgruntled Individuals Employees
- Cyber-terrorism
- Hacktivism
- Protests

[1] Arbor Networks is an American network security company focused on researching, detecting and mitigating network-based threats.

2.1 Cyber Threats And Risks Against Hospital Information Systems

Health information is a very critical asset and should be protected, since hospitals are prone to the risks of data loss or data leaks without a proper network security. Protecting the network from threats and vulnerabilities by keeping a balance between maintaining integrity, protecting confidentiality and assuring availability is of prime importance in healthcare institutions. Vulnerability is defined as a weakness in the system which possibly causes a threat. A threat can be an unauthorized access to a network. By incorporating effective safeguards, it is possible to mitigate the effects of the threats and attack types that will be described later in this chapter. Mainly all attacks target the confidentiality, integrity and availability of networks; but it is possible to classify them according to their source external attacks that target unauthorized access to the network and information; and internal threats that is caused by insiders by ignorance or violation [4].

2.1.1 External Attacks

When an attacker decides to target a system, the first phase is intelligence gathering. This helps the attacker to get prepared for the attack. This may include searching about the target person or organization through the internet, social engineering techniques which will be discussed later in this chapter- and physical dumpster diving methods to get sensitive information that can later be used. Intelligence gathering is followed by Active Scanning, where the attacker tries to identify critical systems and their vulnerabilities. While information gathering can be executed without the knowledge of the target, during active scanning there is a potential for detection. This is followed by the exploitation phase, where the attacker penetrates the system or sometimes even gets access to the systems. Once gained access to the system, the attacker can infect the systems, remove any evidence of his/her existence and get sensitive information[4].

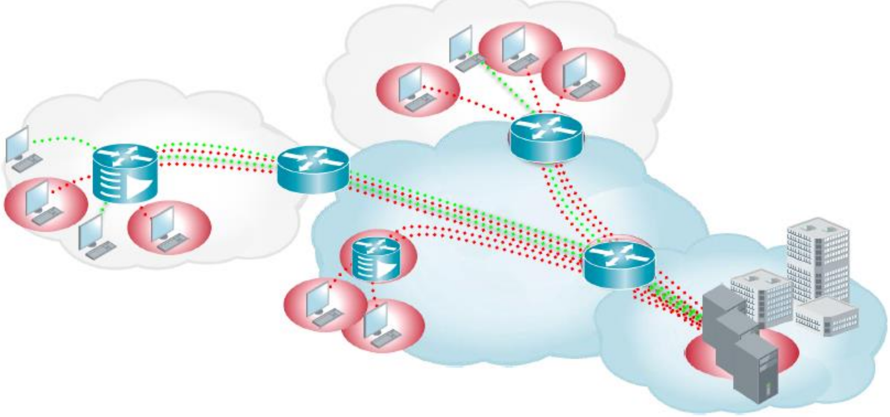

Figure 2.1 Arbor Network's illustration of a DDOS attack [1]. The gray buildings and servers on the right-hand side represent the target corporate. The computers represent the clients sending IP packets to the target server on the corporate. Green dotted lines symbolize the legitimate traffic and red dotted lines symbolize the bad traffic coming to the target server from malicious clients.

2.1.1.1 DOS/DDOS Attacks. Denial of Service (DOS) attack targets the availability of systems and its purpose is to prevent legitimate users to access the systems. DOS attack sends several IP packets to the target system as a flood of packets which then inhibits the server's ability to respond to legitimate users. The word service in the name of the attack can be any feature or capability [5]. Most services affected by DOS attacks are Web, DNS, Email services, Voice over IP (VoIP) applications, network devices and firewalls. DOS attacks have different forms and are very popular because the harm given to organizations after the attack is very costly. Furthermore, malicious users can easily find attacks tools and can use the tools with basic computer knowledge. Botnets and malware is a common technique to perform a distributed denial of service attack. During a Distributed Denial of Service (DDOS) attack, compromised hosts or bots coming from distributed sources overwhelm the target with illegitimate traffic so that the servers cannot respond to legitimate clients. The figure 2.1 shows how a DDOS attack is performed.

According to Arbor Networks 8th Annual Worldwide Infrastructure Security Report, denial of service and distributed denial of service (DDOS) attacks are the biggest IT threats for enterprises. When it comes to healthcare organizations, DOS attacks can target the availability of services such as websites, financial transactions, supply chain, email services. The focus behind DOS attacks are usually data integrity.

While the systems are brought down, information in critical databases can be stolen or even altered to cause another denial of service on the applications and databases.

Arbor Networks classifies DOS attacks in 3 groups:

- Application Layer Attacks, which specifically target an application and sends malformed packets with the help of vulnerabilities or normal behaviors in the protocol;
- State Exhausting Attacks which target the availability of network or security devices by consuming their resources like bandwidth, buffer, memory and CPU;
- Volumetric attacks which target enterprise's internet link capacity temporarily making the network inaccessible to attached devices and real users.

With the rise on web applications, hospitals have started to be victims for cyber attacks. Attacks can target all web applications, internet bandwidth and internet enabled medical devices, which was the case when Veterans Administration (VA) in the USA was attacked on February, 2011[2] . VA is the USA's largest integrated health care system, with more than 1,700 hospitals, clinics and other facilities. VA has experienced illegal intrusions into their medical devices and wireless systems. After analyzing these cyber-attacks, VA has changed the network deployment by moving critical systems including PACS onto a separate network from primary HIS.

2.1.1.2 Social Engineering. Social engineering attacks exploit trust between people by lying or with verbal tricks in order to gain information to get access to systems. This technique usually targets employees of organizations that have information desired by hackers[5]. When the network is securely designed and the attacker cannot penetrate to the system, he/she uses social engineering techniques to get access

[2] "Cyber-Attacks against Internet-Enabled Medical Devices are New Threat to Clinical Pathology Laboratories", Published at Dark Daily on 16 February 2011. (http://www.darkdaily.com/cyber-attacks-against-internet-enabled-medical-devices-are-new-threat-to-clinical-pathology-laboratories-215ixzz35OjuTWRl)

to systems. Hackers send emails to the victims by imitating real emails coming from system administrator, customers or colleagues trying to trick them into sending their passwords for some critical systems or downloading a piece of malicious software which then captures username and password. In order to prevent social engineering attacks, employees need to be trained on social engineering scams; that they should never give passwords to anyone including system administrators and they should not download executable or suspected attachments from people they do not know.

2.1.1.3 Software Exploitation (Malicious Software and Viruses). Software exploitation attacks take advantage of vulnerabilities in software on a computer system. Attackers mostly make use of well-known vulnerabilities. These vulnerabilities are known by public as well as their vendors and vendors make software fixes and patches available to their users/customers. Security patches are usually available free of charge and can be downloaded over the internet. It is suggested to download the latest security patches and run the latest version of software on all critical systems to stop software exploits. Software exploitation may also include malicious software, or malware. A malware can be a software virus, worm, Trojan horse and backdoor programs. All of these programs serve their masters (the attackers) with their negative behaviours by propagating across other computers over the network, infecting legitimate programs, gaining remote access to systems without the permission of its legitimate owner, deleting and modifying files. We will not be providing further detail on the operating logic on these attacks. Besides keeping the systems up to date and having them run the latest security patches, it is also important to have antivirus software with an updated virus signature database. A virus signature is a fingerprint used to detect and block a malware. An antivirus system must also be running the latest version of software and must always have the latest signatures available to protect against the latest malwares.

2.1.2 Internal Threats

Internal threats constitute the large amount of risk when dealing with sensitive information if necessary precautions are not taken. Disgruntled employees can easily benefit from their own access privileges to critical information. However, threats are not only caused by one's own violation; user errors and lack of awareness across stuff also put networks at risk [4].

2.1.2.1 Data Theft / Data Leakage. Stolen or lost laptops are a common breach to sensitive information. Considering the case that the stolen laptop had a copy of many health records and secret documents, the data loss gives harm to the related individual's privacy as well as to the reputation of the health organization. In order to mitigate the risks, DLP (Data Loss Prevention) and hard drive encryption solutions are suggested, so that even if the laptop is stolen, the critical information cannot be read by unauthorized people. DLP solutions are like firewalls to file types on which you can create policies that define who can access to which data. This way, even in the same organization, it is possible to grant access only to limited personnel for some critical information but not to all health staff. An example can be a psychologist who can access to his/her patient's information while other healthcare personnel is limited to access the patient's private records related to psychology department.

2.1.2.2 Unintentional Filesharing. Use of mobile devices including mobile phones and laptops provides flexibility to employees beyond doubt while extending the organization's network boundary without its control [4]. File sharing applications are easy to install and use whether sharing files on LAN or internet through FTP or P2P (point to point) programs. But, the files under the shared location are prone to the risk of confidentiality and damage. There is specific type of malicious code that targets hard drives or network drives, damages the files and inhibits productivity. The solution to remove this risk can be to control the end users and not granting administrative privileges to avoid installation of P2P programs that have the risk of spreading virus and malicious code. Another solution can be using disk encryption on critical drives that have sensitive information so that only users who can decrypt the files can read them.

2.1.2.3 Attacks against encrypted data. Encryption is a technique of encoding a file so that it is only readable by limited and intended group of recipients. Encryption is achieved by giving the original file as an input to a mathematical algorithm and a key; so the output is an encoded file. Vice versa, if the key and the algorithm is known it is also possible to decode the encrypted file to obtain the original file. In the previous types of threats, encryption was suggested as a solution. However, encryption is not enough if the algorithm or the key itself is somehow cracked. Weak keys are prone to vulnerabilities if encryption and decryption uses the same key. Attacks against keys and passwords can involve guessing or cracking computationally by automatic scripts. Mathematical attacks benefit from the weaknesses to decrypt the file or to discover the secrets.

3. RISK MANAGEMENT AND REGULATORY COMPLIANCE

It is often not possible for network administrators to entirely secure everything. However, it is possible to define the critical assets and identify the risks against these assets. For a healthcare organization, the most critical asset for sure is the PHI. In order to mitigate the effects of possible breaches, risk management processes should be put in place in which network administrators and security specialists control the risks, address vulnerabilities and take actions to minimize the effects of threats. It may not always be easy to change and improve processes even if it is for the patient's own good. Although, the ICT, Information and Communication Technology world allows, it is usually possible to apply these technological changes to the common systems only with obligation and the necessity of standards, laws and regulations. Below, we will provide some information on the Healthcare Standards that are applied in US, Europe and in Turkey that specifies the guidelines for the users and administrators across healthcare organizations.

3.1 HIPAA - Health Information Portability and Accountability Act

Legislated and applied as a law in US since 1996, HIPAA, the Healthcare Information Portability and Availability Act, forces the use of uniform electronic records for transmitting and possessing health data in order to make it available and portable [6]. HIPAA covers management of electronic records and the routine procedures for storage systems, backups, software upgrades, access and authorization issues and, most importantly, the security of data being stored. IT aims to protect patient records, named as protected health information by HIPAA. It has a technical checklist for covered entities that addresses network and applications that the health data resides, processed and transmitted. It is made up of best practices and covers suggestions on applications on network design to protect health data; while other standards like IEC 80001 and HSQS focuses only on risks and threats that may be introduced on the systems but not on the solution to the non-conformities. HIPAA basically covers the following major topics:

- Policies and procedures - including security policy, procedures that explain how the data is processes from its collection to disposal
- Security agreements between interested parties
- Information access control and data authorization control
- Physical access control
- Security configuration management
- Personnel security trainings and awareness
- Media controls
- Workstation use, secure logons and inactivity timers
- Unattended device and workstation security
- Logging and monitoring of systems to detect events and incidents
- Verification of data to prevent unauthorized altering of data (integrity of data)
- Communications and Network Controls
- Electronic signature standard although this standard is not mandatory since it is not possible to implement PKI, public key infrastructure signatures in every health organizations due to high costs.
- Incident Management
- Business continuity plans - including disaster recovery plans, emergency mode operations plan, data backup plans and procedures for testing the plans
- Ongoing risk analysis
- Internal Audits

The details of the titles will not be discussed in this thesis since they are publicly available on the web site by HIPAA. Documents on the standards and application of the standard are made available to public on the web site of US Department of Health and Human Services. The documents are easy to reach and understand, also supported by a FAQ, frequently asked questions, section. HIPAA is mandatory across US; therefore the covered entities need to conform with HIPAA guidelines. The entities have to be assessed to examine their security practices against HIPAA internally or by an external agency. If the organization is found to be deficient when protecting sensitive information, HIPAA imposes civil and criminal penalties. In this wat, the assessment and compliancy process is a continuous and ongoing process, which forces the healthcare delivery organizations to identify their deficiencies and sufficiencies.

3.2 IEC 80001 Standard: Application of risk management for IT networks incorporating Medical Devices

Published on 2010, the standard IEC 80001, is adopted internationally by ISO and IEC and also in the USA by ANSI/AAMI (American National Standards Institute/Association for the Advancement of Medical Instrumentation). It has a set of requirements including risk management guidance, medical device security needs, risk and controls, guidance for wireless networks and general implementation guidance for Healthcare Delivery Organizations [7]. IEC 80001 has been prepared by referencing standards and frameworks like NSA, IETF, SANS, WEDI, IHE [7]. The goal of the standard is to maintain the safety, effectiveness and data security when connecting medical devices to hospital IT networks. The standard focuses on the risks and risk management processes giving examples on high level actions that hospitals should undertake. The standard tries to address possible risks from implementation to discontinuation during the lifecycle of the medical device or the entire IT network. The standard necessitates top management's support; the management is totally responsible for defining the policies and procedures and also for ensuring that they are applied. There has to be a coordination between internal departments, medical device manufacturers and IT vendors. This coordination is the role of risk management coordinator in order to ensure a safe, secure and effective network while the electronic data is being collected, processed or transferred. Moreover, there are also responsibilities for vendors. Both the medical device manufacturers and the IT device vendors also including the software vendors- shall provide technical specifications to the hospital for correct configuration and commissioning. They need to document security requirements and any known constraints or incompatibilities. In order to ensure that all stakeholders and third parties are aware of their roles and responsibilities, contracts and non-disclosure agreements (NDA) shall be signed in-between describing the service or product. By implementing the standard, hospitals initially can gain improved communication between interested parties. In order to ensure data and system security and operational efficiency, any possible risks will be documented, analyzed, evaluated, managed and minimized; which thereby ensures patient safety and security. The standard specifically covers many risks and how they can be mitigated by also giving examples on threats and risk management. For instance, IEC 80001 gives specific examples on medical devices connecting to wireless internet. However, this standard is not mandatory until it is endorsed by a regulatory organization so it is currently a voluntary standard which will help health organizations to improve their operational efficiency and system security.

3.3 HSQS : Hospital Service Quality System

Ministry of Health in Turkey has designated its quality criteria in 2005 in a project that aims improving institutional performance and quality [8]. The criteria which constituted of a checklist of 100 items has evolved and come into being Hospital Quality Standards in 2008 with a set of revisions. The standard, known as HHKS in Turkey, has been published in 2009 officially. HHQS has 3 main areas including corporate services, health service management, support services, focusing more on patient and employee safety rather than security. Information management is a part of support services and covers only IT devices and does not even mention medical devices incorporating the IT networks. When the information management section of the HSQS standard is compared with IEC 80001 and HIPAA, it is more like a quality management system rather than being an information security standard. Regarding the Information Technology perspective, HSQS focuses on the following items:

- All the records should move from paper to electronic records and must run on the different modules of the same single HIS software.
- An inventory of all information systems including hardware and software components is mandatory.
- There has to be an antivirus software running on all computers and servers.
- Database activities and logs regarding the application have to be logged and monitored when required.
- Access requirements shall be defined and documented.
- System rooms shall be secured with physical access controls, routine maintenance, with uninterruptable power supply and generator.
- A team responsible for HIS software problems has to be specified and problems regarding the HIS software shall be recorded and resolved.

4. METHODS

4.1 Review Of Risk Management Standards

In this study, a checklist obtained from NIST (National Institute of Standards and Technology) is edited according to the procedures in healthcare with the help of standards HIPAA, HSQS, ISO 80001 and ISO27001 details of which is not discussed in detail in this thesis but forms a basis for ISO 80001. Some general concepts already overlap on each standard which are also generic to many industries. However, we have tried to focus on protecting personal health information. The control objects then covered the following entities:

- Security policy
- Asset management
- Physical security
- Access control
    1. Password controls
    2. Network Access
- Communication and operations management
    1. Controls against malicious code and viruses
    2. Controls against Firewall
    3. Controls against critical databases
    4. Encryption and Data Loss Prevention
    5. Application Security
    6. Wi-Fi Security
    7. Medical Devices with Internet connection

8. Mobile Devices

- Information Systems routine maintenance
- Disaster recovery and business continuity

While interpreting each issue above, we have made use of COBIT framework which is very commonly used in finance industry and can easily be applied to any company from other industries. COBIT is not a standard but a framework focusing on controls, risks and solution recommendations to problems[9]. Each clause we have audited is discussed deeper below and the audit results are given in Chapter 5 Audit Results.

4.2 IT Security Audit

4.2.1 Security policy

Every organization that is processing confidential information shall ensure it has a security policy and a team responsible for IT Security in the hospital[8]. The IT Security team is expected to;

- understand the current situation in the hospital
- identify possible risks
- monitor authorization changes across users
- take preventive and corrective actions when necessary. HKS

Moreover, all staff shall be trained according to the hospital information security policies. Our case started with querying if the hospital has rules to ensure information security in the hospital. Unluckily, no written policies were in place prescribing information security policies throughout the hospital. According to BSI, HEALTH DATA confidentiality and integrity is maintained during data transmission between nodes where strong policies are in use[7].

4.2.2 Asset management

According to ISO 27001, an asset is anything that is valuable to the organization. As mentioned in the first chapter, for a hospital, the critical asset is the personal health records. Employee information and financial records can also be considered as assets for an health organization. After assets are defined, the organization has to define

- the asset owners who have the responsibility to manage the asset,
- risks and threats against these assets,
- any vulnerability that causes a weakness for the defined threat to attack the system,
- possible effects in case one or more of the confidentiality, integrity and availability of assets is lost.

It is not enough to define the risks. It is also necessary to classify and rate the risks. Some of the risks may be acceptable if they are rated as low-risk. But some need to be compensated by taking necessary actions. Risks originated from third parties can be transferred to the related parties. ISO 27001 ensures that the organization takes necessary control actions in order to secure the assets, trains the staff accordingly to ensure awareness, detects security incidents and apply preventative and control actions as a response to incidents and improves the management system continuously. During our audit, we have found out that there was no information security management system applied in the hospital. Therefore, the management is not aware of the risks and threats against their assets.

4.2.3 Physical security

According to BSI's ISMS, physical access to secure areas shall be limited only to authorized individuals and equipment in less secure areas shall be physically secured. We have observed that the hospital has employed physical security staff and the hospital is being monitored with 7x24 video recording including system room in case of invalid physical access and data theft. IT Manager informed us that the video records are stored for 1 month and start to overwrite on the oldest data when the 1 month repository reaches. Computers running EHR systems are shielded from unauthorized viewing.

4.2.4 Access control

According to Information Security Management Systems, risks against procedures in accessing and processing information shall be evaluated. Both the hospital staff and third parties shall be assessed for only required and necessary authorization. Users need to access to information which they need to know in order to perform their jobs. This authorization to access information and systems shall be terminated when the employee quits job or the contract between the third party and the hospital expires. Information Technology General Controls (ITGC) suggests that personnel who are still actively working, who began and quit yearly are available. Creating, deleting and changing a user profile shall be clearly defined. BSI suggests if a system is left idle for a period of time, user sessions need to lock after a predefined duration of time. This ensures the risk for unauthorized access to PHI is reduced when an authorized personnel leaves the workstation without logging out or locking the display or room. Our audit results showed that every user has a unique account. When the user quits job, his/her account is manually disabled. There are restrictions on file server for every department so that only authorized personnel can access to files. However, IT personnel have privileged rights and have access to every location on the file server and EHR application. A good observation was that computers running healthcare related systems were restricted to chat and social media websites and health staff does not have local admin rights on PCs. These PCs are configured to lock session if the user is idle for 15 minutes which is another positive observation. Hospital has the capacity and possibility to show the active and non-working personnel list and the procedures are clearly defined to create or delete a user account.

4.2.4.1 Password Controls. Password policy is part of access controls. The organization shall have a password policy similar to the security policy, that it prescribes password practices. According to this,

- Each user has a unique username and password.
- Passwords are private information for every user and are not shared with others.
- Passwords are not written down or displayed on screen.
- Passwords are complex which include a combination of upper case and lower case letters, at least one number and at least one special character. (A strong password is at least 8 characters in length.)
- Users are forced to change passwords routinely.
- Passwords are not re-used.
- Any default password that come with a product are changed during product installation.
- Any devices or programs that allow optional password protection have password protection turned on and in use.
- Single sign-on and same passwords are available for each user on all workstation.

During our audit in the hospital, we have observed that there is a password policy which the staff/employee signs when they start the job at the hospital. According to this, they agree that they do not share passwords with others. The IT administrators change the passwords routinely and it is not possible to re-use the last password after it expired. However, devices that come with a default password like routers or switches in the system room- are left with default passwords. Hospital has not yet officially deployed mobile devices so they are not handling smart-phones or tablets yet. For the health staff, there is only one single password for all applications which is called single-sign-on (SSO). But, the IT staff looks more privileged. They have different administrator passwords (like generic accounts) beside their domain accounts, which is a gap for information security. For instance, if an administrator leaves the job, he/she still has the password for a critical system because the admin account is a generic account which is also used by other administrator in the hospital. If he were using a domain account for all operations, his domain would be locked after he quits job. So he would not have access to any system after he leaves.

4.2.4.2 Network Access Controls. Access to the hospital network needs to be restricted to authorized users and devices only. Guest devices, such as mobile phones and tablets, need to be blocked from accessing networks containing PHI. It is a good practice to limit computers in the network so that they do not contain peer-to-peer applications and no public instant messaging services are used. If necessary, private instant messaging services can be considered but they need to be secured and logged appropriately. Wireless networks have to have encryption. During our audit in the hospital, we have observed that there is no corporate wireless network in the hospital. Neither public nor private instant messaging services are used. Peer-to-peer applications, remote file sharing (including remote printing) and all social media applications are disabled. Hospital has a Wi-Fi for guest networks and it is separate from corporate network. Users (guests) log in to the Wi-Fi via SMS authentication which is another good observation.

4.2.5 Communication and operations management

The purpose of a management system is to ensure sustainability of the services. Every operational procedure has to be clearly defined, documented and made available to the responsible people. If there are any changes in any of the procedure, the updated information has to be shared with the related people. The main goal has to be to protect the organization's assets, which in our case is PHI/EHR, from being changed or from any malicious purposes. It is important to segregate duties so that responsible personnel can control each other and cannot act without the approval of another.

4.2.5.1 Controls against malicious code and viruses. Information Security Management Systems including the draft HKS in Turkey, suggest that all the computers shall run an antivirus software controlled by a centralized management software. Staff shall be trained on how to recognize possible symptoms of viruses or malware on computers [8], [10]. If there are mobile devices like tablets and/or smart phones, they need to have antivirus software installed on them. We have observed positive impact during our audit in the hospital. They were running an antivirus software which the IT administrators are able to manage centrally. The antivirus client is set up to receive automatic updates from the manufacturer. However, there are no policies defining the use of antivirus software and that the users shall not disable or uninstall antivirus software.

4.2.5.2 Controls against Firewall. Today firewalls are almost a must for every organization who has access to internet. All computers and devices must be protected by a properly configured firewall. Unused ports and unused services has to be closed and only necessary IP addresses have to be allowed on firewall. Security on medical devices and software applications can further be hardened, while maintaining only intended use. We have observed that hospital has one layer of firewall on the network perimeter facing the internet. Although the EHR application is web-based they do not have a web application firewall; but limiting access with limited static IP and username matches.

IT Manager also mentioned that they are using operating system based firewall on user machines. The user's do not have local administrative rights on their PCs so it is not possible to disable firewall on operating systems. Our suggestion would be to use a web application firewall since the EHR application is a web application to provide a second layer of firewall security to maximize the protection on PHI.

4.2.5.3 Controls against critical databases. All standards agree that integrity of health data has to be assured. Health data cannot be changed or destroyed. There has to be a strong authentication for accessing databases containing health data. If possible, there has to be authorization rules based on internal and external factors, such as IP address, time of day, application being used and authentication type. Critical table spaces and columns can be encrypted or masked when accessed by unauthorized personnel. E.g. While accessed by a a technical support engineer or a third party manufacturer during an application development test. HKS suggests that separation of duties has to be defined. Users have to be limited to accessing data that is within their clearance level. Every connection, query, change or delete action on the database has to be logged. Moreover and more importantly; administrators and super users for databases have to be defined clearly and their activities have to be logged and monitored. It must not be possible to delete any logs regarding activities on the database including database and system administrator access. Passwords for every user have to be encrypted. If possible, real-time alerting and reporting can be put in place to avoid rule violations. During our audit, we have noticed that doctors have the privilege to change health data. Good thing is all activities are being logged and logs cannot be deleted. There is no encryption or masking in use for health data. But user passwords are kept encrypted. However, doctors and all health personnel are limited to accessing data only within their clearance level. Though, this is not valid for technical IT personnel. Database administrators have the right to access any health data. Every activity on the database and application are being logged. However, logs are not being monitored real-time. There is no real-time reporting or alerting. This means they cannot notice immediately if there is a policy violation. But if they later notice or suspect there is a violation, they can investigate the logs for postmortem activities. Real-time monitoring and alerting is very critical when working with critical data. Hospital's own system administrator and database administrator cannot delete any logs regarding database and application activities. However, it is an important non-conformity that the manufacturer itself has the privilege to delete logs on the database, which is unacceptable. A third party can access the most valuable asset on the hospital, they can intrude on the integrity of health data by deleting or changing it and they can then delete their own activity logs which will cause that they can never be disclosed.

4.2.5.4 Encryption and Data Loss Prevention.

Health information is the most critical asset stored in databases. Therefore, critical information stored in databases and applications can be considered to be encrypted while in use and at rest. Staff shall not be able to copy or record patient information on an unauthorized medial including personal mobile devices, laptops and portable media such as external disks. Patient information is shared with third parties such as insurance companies. While sending health information, only required information has to be shared and fields, that the third party is unauthorized to see, have to be encrypted or masked. Similarly, patient data has to be masked or made unreadable by technical support engineers or any third party manufacturer. During our audit, IT manager has informed us that users access the applications and data only with passwords and passwords are stored encrypted. However, health data is neither encrypted nor masked; and administrators have access to any value. In order to avoid, copying of the health information on user machines, USB ports are locked for use. Unfortunately, patient admission personnel besides IT administrators have access to all fields of the health information like patient appointments, clinical data and laboratory results; which again needs to be limited to patient admission information only. However, this staff is communicating with insurance companies because of their roles and thus, they are granted full access. Data transfer between insurance companies and hospital has not yet totally moved to electronic media. Although there are companies which make the data transfer on their web applications through internet, some companies prefer data transfer via fax and some even acquire the patient information on the phone. Another important point to note; hospital has a level of patients, which they name as VIP patients. This class of patients can be political people or famous people. If these people like to hide their health information, it is possible to mask their names by giving pseudo names. It is very important to understand that every single patient has as valuable information as a political person and no prioritization has to made.

4.2.5.5 Application Security. Every user account has to be tied to an authorized application module. All active users that are authorized to use the application and non-active users that quit working for the hospital are documented. Besides, administrator users that are authorized for the application are documented. Users need to be trained that they are authorized to access data within their clearance level and are prohibited to share data with authorized personnel. We have observed that every user account is tied to a specific EHR module. However, this is only valid for the health staff. IT Personnel has access rights to any module. It is possible to list the active personnel and their authorization levels on the EHR application. Health staff is trained and aware that they are not allowed to share data with unauthorized personnel. However, no special conditions are defined for technical staff like IT administrators.

4.2.5.6 Wi-Fi Security. For hospitals that implement wireless networks, there are some important settings that they need to implement. The most important one is implementation of a QoS (quality of service) policy so that high priority traffic is not interrupted by lower priority traffic. This is highly important where medical devices with Wi-Fi access are in use. BSI suggests that a clinical transport policy is created for hospitals that have medical devices for wireless patient monitoring during patient transport. Locations with higher wireless traffic have to be identified and WAPs (wireless access points) in those areas have to be increased if necessary. Roaming has to be implemented on WAPs so that connection will not be lost during patient transport. Microwaves have negative impact on wireless signals. BSI suggests that if there are any microwave ovens, hospitals have to consider lower emission microwave or implement the necessary RF shielding[11]. Guest wireless network has to be separate from hospital's wireline or wireless network. As an increased security, access to guest network has to be logged. During our audit, we have observed there is no medical device with wireless access. Hospital has also not implemented a wireless network for internal use. They have a guest wireless network separate from hospital's network. Users need to enter their mobile phone numbers to get a password which then provides access to guest Wi-Fi. Network connections of guests are logs according to Turkish Law 5651*.

4.2.5.7 Medical Devices with Internet connection . Medical devices have to be configured only for the intended application and network design has to be implemented according to this by means of IP address, speed/duplex settings, planned storage, next hopes, etc. They need to be designed in a separate IP network. They need to be updated or patched regularly as suggested by the manufacturer. If possible, antivirus software has to be installed on devices with internet connection to avoid malicious access. A network monitoring software can be used to monitor medical devices with internet access. We have observed that the hospital has not implemented a separate VLAN for medical devices. Furthermore, they are not monitoring the devices. Every manufacturer is monitoring their product through a specific port. Hospital does not have medical devices with wireless access, like wireless patient monitoring, remote ICU or Post Anesthesia Care Units. Therefore, precautions for wireless access are not applicable. However, they still need to harden security since they have devices with wireline internet access. They need to consider manufacturer connections by means of limited time. So that manufacturer's cannot get access to network whenever they want. Devices are patched regularly by manufacturers to avoid degraded function but unauthorized access is still a problem. If the devices were to be monitored by the hospital staff, they would take the necessary precautions in case of an alert or an anomaly in the network traffic to avoid loss of availability. However, when devices are monitored by manufacturer, they will only take care of their product's resource since the rest will not be their responsibility.

4.2.5.8 Mobile Devices . According to HIPAA, if there are mobile devices like smart phones or tablets that have access to PHI, it is a must to implement authentication on these devices to prevent unauthorized access. The devices have to be password protected so that if the device is left idle for a period of time the screen is locked with the password. The PHI data on the device has to be encrypted. Moreover, connections between mobile devices and EHR application are encrypted. A security software like antivirus software has to be installed on mobile devices. File-sharing and peer-to-peer applications are not allowed, as they are also not allowed on desktop computers. In case of theft or lost device, mobile devices have to be wiped remotely. When the device is returned to manufacturer for any failure or if it is handed over to any other user, all the health information on the mobile device has to be removed. The hospital we have audited does not implement mobile devices officially. Therefore the precautions mentioned in this section are not valid for them.

4.2.6 Information Systems routine maintenance

For the purpose of the availability and integrity of the whole system and service, it is essential to make the routine maintenance of the devices correctly and in a timely manner. Besides, staff with responsibilities for maintenance has to understand and agree to system maintenance procedures. All vendors and third party companies have to be documented clearly with up-to-date contact details. Vendor remote maintenance connection details have to be documented and fully secured. A change management procedure has to be clearly defined. All systems and applications need to be updated and patched as recommended by the manufacturer. Users of application or database needed to be notified when a system upgrade or patch will be applied. Test and live environments have to be separate, so that when a new software version is available, it is first tested on the test environment and live system is not affected of the new software has some software bugs and is malfunctioning. In case of a fault or failure, case management procedure has to be defined and staff with responsibilities has to understand and agree to procedures. Users need to know whom to contact in case of a technical problem. These technical cases need to be documented which later provides faster response times when the same issue happens later again. During our audit, we have noticed that the hospital does not have a written change management and case management procedure. However, they are still trying to manage device maintenance with the help of vendors. Both network devices and medical devices are being patched and maintained by manufacturers of the related devices. Manufacturers are connecting to the hospital network with VPN connection. Unfortunately, no security precautions are taken for remote connections. There is no limitation for the time that they will be connected, no token and no logging. They have non-disclosure agreements with the manufacturers which they trust. After the maintenance, the changes are being documented. Unluckily, there is also no control on the critical data that the manufacturer can access. When the device is shipped back to factory, information on it is not removed. So, if there is any identification of patient, it is exposed to the service engineers at the manufacturer. This issue is very important and we believe that any precautions should be taken by the law. There is currently no control when and how the manufacturer gets access to the hospital network. They are also not aware of the risk if the service engineer at the manufacturer leaves his/her job; since he/she still knows the password, he/she can still get access to critical systems. Since there is no logging, no control and limitation of time, it is not possible to identify the bad guys. Hospital of interest, has a case tracking system and user problems are reported and resolved via this tool. The date when the problem occurred, how and when it was resolved are all documented for future reference. However, critical systems and medical systems are managed by the manufacturers as discussed before. Therefore, hospital does not have a test environment separate from the live environment.

4.2.7 Disaster recovery and business continuity

Organizations which process critical information shall have a recovery plan in case of emergency and disaster; and staff who has roles in recovery plan shall understand their duties during recovery. Hospitals, as they process critical health data, must also consider a recovery plan. According to this,

- System restore procedures are clearly defined.
- These procedures are known to at least one trusted party outside the practice.
- A copy of the plan is safely stored off-site
- Backup schedule is timely and regular.
- Temperature and humidity of the system room containing devices for PHI and critical health applications are monitored real-time.
- System room is insulated well against water.
- Devices for PHI and critical health applications are connected to a generator and a UPS (Uninterrupted Power Supply) separate from other UPS devices in the hospital.
- Backup is stored in a different platform where the HIS is running, even off-site if possible.
- Every backup run is tested for its ability to restore the data accurately.
- Multiple backups are retained as a fail-safe.
- While transferring backup data out of hospital/site, sending site and receiving site ensure a signed proceeding
- Application servers are running High-Availability (active-active or active-passive) to ensure application redundancy.
- Backup media are made unreadable before disposal.

During our audit, we have observed that the hospital does not have a disaster recovery plan. However, they are planning to implement a monitoring system in the system room in order to monitor temperature and humidity that will give alerts if the values are out of the optimal range. There are currently 2 generators and 1 UPS in the hospital. System room is said to be insulated well against water. There are 3 application servers working in high availability mode and 2 database servers. Another good observation is the daily backups of the databases. They are also testing the ability to restore from backup and recording the test results. However, backup media are not physically stored, only online and systems are not geo-redundant which is acceptable as they have currently only one hospital in Turkey. Working with a datacenter for redundancy purposes can be considered in the future.

5. AUDIT RESULTS

The objective of this assessment was to assess the status of the compliance of the hospital to information security related items addressed in healthcare standards HIPAA, ISO 80001 and HSQS as well as common items in ISO 27001 Information Security Management System which can be applied across any organization from any industry. Our findings are classified into three as non-conformity, observation and good practice.

Assessment was based on sampling and declaration of the staff, therefore there can be non-conformities that were not identified.

5.1 Nonconformity 1: No security policy is in place

Current situation: No written policies were in place prescribing information security policies throughout the hospital and no risk assessment was performed. According to BSI, HEALTH DATA confidentiality and integrity is maintained during data transmission between nodes where strong policies are in use [7].

Risk: Without having a well-defined policy, there is a risk that users and management personnel may not be aware of their roles and responsibilities in case of security breach incidents and the hospital may not be able to react and recover from the situation in minimal time.

Suggestion: A security policy describes the strategy on protecting the hospital's most critical assets in normal conditions and also in cases of security breach incidents or disaster events. In order to set up a security policy, the hospital needs to list what is critical for them, where on the system this critical information resides, what other assets the hospital has, what risks these assets face, what actions need to be taken to minimize and manage the risks, the responsibilities and the personnel in charge of the actions to be taken. After the security policy is defined, it should be communicated to the users, management and to patients where necessary. E.g. hospitals can communicate their security and privacy policies on their web pages and physically on notice boards.

5.2 Nonconformity 2: Asset management has not been performed and no asset inventory has been established.

Current situation: It has been seen that the hospital has not identified a list of its assets, where these assets reside and the owner of the assets. Thus, they do not know the significance level of the assets for the business to continue and the severity that can be introduced in case the asset faces a risk.

Risk: Without having an asset management policy, the hospital has the risk of not having control of the asset inventory. Therefore, the hospital will not be able to manage the life-cycle of its medical and IT equipment as well as other critical and supportive electrical equipment like UPS, generator and air condition.

Suggestion: An asset is defined as an item of importance for an institution which can be a physical item like a laptop, a server, a storage system or it can also be information in a database like PHI or financial information. The organization, that is the hospital in our case, has to identify all the assets it has; the owner of each asset, where it resides in the hospital; and reiterate this process of asset review yearly. This will help the hospital to have a full control on its assets by means of cost and risk by enhancing the availability of the asset and the process; so that if there are any assets that are no more available for use will need to be renewed improving the performance.

5.3 Nonconformity 3: There is no team responsible for Information Security in the hospital.

Current situation: It has been told that the there is no human resource dedicated for information security across hospital. No one is responsible for information security incidents or security trainings across hospital.

Risk: Without having a dedicated information security team, it may not be possible for the hospital to implement any information security related management system or to ensure compliance to laws and regulations. It may not also be possible to train the staff and prepare processes and procedures for information security.

Suggestion: The starting point of implementing information security to the processes throughout the hospital shall be establishing an information security team which can be built up of IT, quality, operation personnel with the support from management.

5.4 Nonconformity 4: There is no strong password policy.

Current situation: It has been seen that there is no password policy applied across hospital information systems. Users are allowed to select weak passwords. Moreover, IT systems were not domain controlled and there was no single sign-on (SSO) for network and security devices.

Risk: The risk for weak passwords for users is that these passwords can be cracked or obtained by malicious persons. This brings the risk of gaining access to critical systems by hackers or malicious users. On the other hand, the risk of not managing the network devices with single sign-on, is the inability to disable the account in case the system administrator leaves the job. So, even though broken off, a user with full access to HIS system and database will still have access to the personal health information, credit card or insurance information of patients, database for salaries, employees and any other financial or secret information.

Suggestion: As a best practice, strong policy should be at least 8 characters in length and include a combination of upper and lower case letters, numbers and special characters. The users should be forced to change passwords periodically, for instance once every 3 months. This strong password policy should be applied across any IT system that requires a log on. If possible, single sign-on and same passwords should be made available for each user or administrator on all work spots. This ensures that when user quits job and his/her account is disabled, all related access rights will be disabled as well.

5.5 Nonconformity 5: There is no segregation of duties on servers and database for IT administrators

Current situation: IT administrators have excessive system access to HIS application and also to the database containing health information and payment information which are private to any individual.

Risk: IT personnel neither provide treatment or healthcare services to the patient nor collect payment from the patient. Sensitive information is left visible to users who are not appropriately authorized by the patient or patient's legal representative to see the personal identifiable information. No single user should have excessive privileges that bypass checks[12].

Suggestion: Personal identifiable information in the databases can be masked or encrypted so that only users who are authorized to work with the data, like healthcare staff, can see the data but other users like IT personnel cannot see the personal information of patients, like social security IDs, name and last name, patient history, credit card numbers, address and phone numbers. A database firewall can encrypt the selected fields of the database; or a script or a software program running on the database can hide the PHI from unauthorized view.

5.6 Nonconformity 6: There is no change management policy.

Current situation: The hospital does not have a change management policy and there is no awareness for the need for a change management process.

Risk: Implementing changes to the live environment incorrectly can lead to security breaches or negative impacts on system's continuity and availability.

Suggestion: Changes to the processes, facilities, hardware or software systems that affect information security should be under control and should be performed on a planned basis[13]. All major changes should be documented, discussed with the responsible people and tested before implementation. So that, changes do not disrupt the normal operation of the IT systems, do not affect the hospital to provide the services or do not cause any security breaches. Change management process should be documented and the document should include the types of changes, like software upgrades or modification to the hardware. When a change is necessary, the responsible person should enter a form including information like the type of change, its possible impacts and the implementation date planned. Moreover, a committee of users should meet regularly to discuss the submitted changes and the risks that may be introduced on the living system. The change request should be accepted or rejected according to the risk analysis; therefore should be implemented or put on hold for further work.

5.7 Nonconformity 7: Manufacturer of the HIS application have full access as IT administrators and can access to PHI.

Current situation: The HIS application used across the hospital is an integrated solution with many modules used across different departments and is manufactured by a local company upon hospital's requirements. The software support was given by the manufacturer itself. The manufacturer has remote access rights to the hospital network and can access the database behind theHIS application which contains all information regarding the patients including their health history and personal information.

Risk: Manufacturer is not authorized to see the patient's PHI but is responsible for the maintenance of the application, its modules and the hardware that the application is running on. Similar to the nonconformity 5.5, information is left visible to users who are not appropriately authorized by the patient or patient's legal representative to see the personal identifiable information.

Suggestion: masking/encryption and limited access to 3rd party The information in the database should be protected from unauthorized view. The third party companies should be provided limited access within their requirement level. The selected fields in the database which contain PHI should be masked or encrypted so that only users who are authorized to work with that data can view the data as decrypted.

5.8 Nonconformity 8: Manufacturer of the HIS is capable of deleting the logs for activities he performed on the live system.

Current situation: Manufacturer of the HIS application has full control over the live HIS system and the database behind it where the patient data resides; and capable of deleting his own activities on the system.

Risk: With full administrative rights on the system, the manufacturer can manipulate, delete and add any data to the live system. Although, these activities are logged on the system, manufacturer also has the right to delete any logs which lets him not leave any traces behind him after a security breach or a data loss.

Suggestion: The manufacturer, although intervenes in the technical problems of the software or the hardware, is not the owner of the data. Therefore, it should be given only limited access to the critical information. All activities performed on the system should be monitored with extra controls on external logging systems. Therefore even if the logging on the system itself is deleted, its copy on the central logging system still captures the events.

5.9 Nonconformity 9: Test and live environments are not separate.

Current situation: There is no isolated environment in order to test applications before it is implemented in the live system.

Risk: If there is an upgrade, configuration change, device replacement or if a new device or software will be implemented to the live system, technical defects can occur and impact the production environment. Functionality and availability across many departments can occur and the service can be adversely affected.

Suggestion: A small and isolated environment can be established which is a simulated network of the real environment. Before a software change or a hardware change is implemented, the change first should be tested on the test environment in order to verify that the live system will not malfunction after the change.

5.10 Nonconformity 10: There is no NDA between hospital and manufacturer.

Current situation: The hospital IT manager has explained that the maintenance and repair services for the database, HIS/RIS applications, the hardware systems that the HIS/RIS is running on and all medical devices were each handled by their own manufacturers where necessary. CT, ultrasound, ECG, EMG and Patient monitors in intensive care units and clinics are periodically maintained by the Biomedical department for routine maintenance and calibration with simulators. When required, remote access settings are enabled by approval from Biomedical Department and the vendor is capable of remotely connecting, monitoring and giving support. But it has been observed that there is no non-disclosure agreement between the hospital and the manufacturers.

Risk: The purpose of the service and the limitations of what may and may not be done when dealing with the network have not been specified. Any malicious employee from the manufacturer or the third party company that provide service can gain access to and abuse the sensitive information. The extent of obligations and the action plan upon a security breach have not been established.

Suggestion: A non-disclosure agreement is a contract signed between two parties when confidential information is shared in-between. Since PHI is confidential for each and every patient and all the devices incorporating medical data is of great importance for the continuity and confidentiality of the service, requirements protecting the sensitive data should be entered into the NDA. The benefit of an NDA is that the hospital can sue the other party in case of a security breach.

5.11 Nonconformity 11: There is no real-time alerting and monitoring of the systems.

Current situation: There is no monitoring for the alerts that can occur on the network and security devices to view performance or alarming events. It is not possible to identify the anomaly in the traffic or high usage of the resources like CPU, memory, hard-disk or bandwidth.

Risk: If the systems are not monitored, it may not be possible to detect security attacks against the systems, identify already compromised system's, gain visibility on performance of systems, identify failures, monitor availability of services.

Suggestion: Hospital network, computer systems and servers should be monitored to validate the effectiveness of the controls and gain visibility over the entire architecture[14]. Monitoring also ensures that problems are identified quickly and resolved with immediate actions before the issue gets worse.

5.12 Nonconformity 12: Medical devices are not configured for a specific VLAN.

Current situation: There is no segregation in the healthcare network and all IP enabled devices including medical devices exist on the same network.

Risk: Employees of third party companies providing maintenance services for medical devices can gain access to the sensitive information. Moreover, any malicious activity on the network can impact all devices residing on the same network which can be disastrous.

Suggestion: A layered approach can be implemented across hospital network[10]. Each department like clinics, inpatient/outpatient, reception/accounting and radiology should have a separate VLAN. HIS application server, the database behind it, others servers including email and web server can be all in a data center network and even more segregation can be done inside this network. This approach helps to eliminate the risks of undesirable network intrusion attempts if any of the systems is breached. Even if the attack to one of the separated networks is successful, the negative impacts will be limited within the segregated area and will mitigate the risk of infecting other machines.

5.13 Observation 1: HIS Application is not domain authenticated.

Users are provided two different username and passwords, one to log in to the workstations and the other to log in to the HIS application. Same is also valid for IT administrators when they are logging into the servers, network and security devices. They have one set of user credential when logging in to their PCs or laptops, and one set of credential for each IT system they manage. HIS application is used by almost all departments except physical security, nurses, technicians- and has many modules including patient admission, clinical modules, laboratory, pathology, radiology (RIS), device inventory, stock tracking and payment modules. There are 334 users on the system and every user is manually generated on the HIS application's user management module. When the user quits the job, his/her accounts have to be disabled manually on both systems. As a best practice, the hospital management can consider an improvement to use single sign on every system that requires password. In that way, in a scenario where the user quits the job, it will be easier to manage the accounts. Integrating the systems that require a user log in to an LDAP server can be considered. An LDAP server stores the users, their roles in the organization and their passwords. So, when a user sends his/her username and password to log into one system, that system queries the user credentials on the LDAP server. If the LDAP successfully authenticates the user, the system requiring the password returns OK to the user and the user can log in. The advantage of using an LDAP server is reducing the workforce

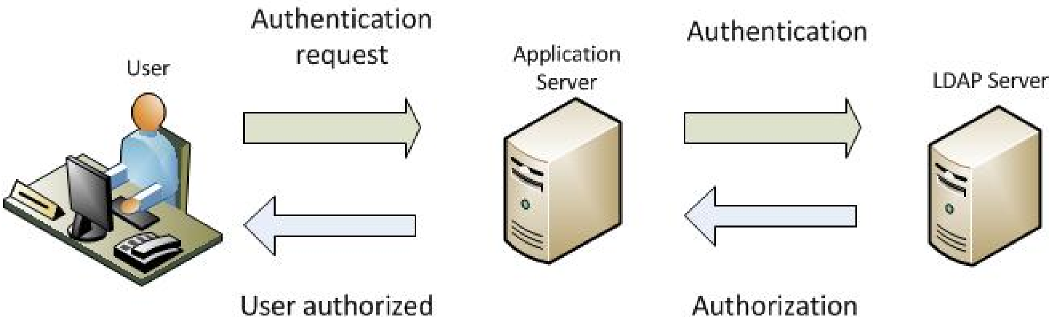

Figure 5.1 How LDAP authentication works. 1.The user makes a request to login to the application server. 2. The application server send the request to the LDAP server to query the existence of user. 3. LDAP server controls if the user exists and if the password is true. 4. If the username and password is verified, LDAP server sends an authorization approval to the application server. 5. Application server authenticates the user. (If the username or password are not correct, LDAP server does not verify the user and application server rejects the user.)

on administrators when activating new accounts or when disabling the old or unwanted accounts. Disabling the account on a single system the LDAP, will de-activate it on every system where the same credentials are used. Another advantage would be the simplicity provided to the users, so they do not have to remember so many passwords. Finally and most importantly, it will be much easier to track the user on every system log with one single username in cases of security incidents or undesirable events.

5.14 Observation 2: No offline or off-site backups of databases.

The databases containing health data and the HIS application servers are backed up in a timely and regular manner. Hospital Service Quality Standards obligates that health data should be backed up off-site and the backup media stored off-site should be encrypted. We have observed that the database is backed up every night on the disk of same hardware that the live system is running. Besides introducing extra performance load on the server, with this deployment, if the server is physically damaged by a fire, flood, earthquake or any other disastrous event, it may not be possible to recover the data.

Similarly, the backups of HIS application servers are not stored on a different platform. The application servers are running in high-availability (HA) mode. So, if

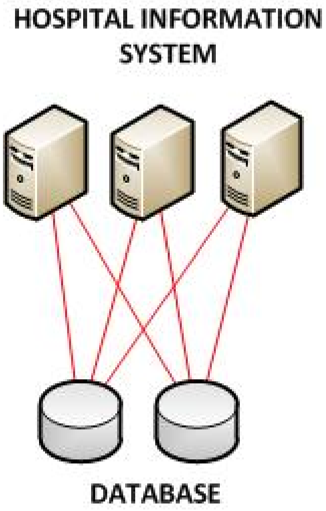

Figure 5.2 HIS Application Servers with redundant links to 2 Database Servers.The Application Servers and Database Servers are both running in High Availability mode.

one server is not active for any reason, the other server will preempt and take the load. However, if the applications are physically lost for a disastrous event, it may not be possible to reinstall the application. Hospital Service Quality Standards obligates that backup is stored on a different platform where the HIS is running, even off-site if possible. In our case, the backup of each application server was stored on the other server; which does not really reduces the risk.

5.15 Good Practice 1: System room is planned to be monitored with a monitoring system.

The hospital IT was in the process of purchasing a monitoring system which will continuously monitor the temperature and humidity in the room and notify the responsible persons if the measured values are not within accepted levels.

5.16 Good Practice 2: Limited user privileges on workstations that run healthcare related systems.

IT department has given only limited access to healthcare staff and reception personnel on PCs. Standard users do not have local admin rights on the workstations that run healthcare related systems. Only IT staff can access the workstation with administrative rights in order to provide support service where necessary.

5.17 Good Practice 3: Idle timeout on workstations that run healthcare related systems.

IT department has successfully implemented idle time out on user workstations so that after a period of inactivity the screens are locked with password. If a workstation is left idle for 15 minutes, the user session is automatically locked and he/she has to re-enter the password. This reduces the risk of unauthorized access to health data on unattended systems[7].

5.18 Good Practice 4 : Guest wireless network cannot access to health data.

All legal communication and network traffic across the hospital is carried out through wireline. Wireless network is only broadcasted for guests and it is separated from hospital's HIS network. Thus, guest devices are prohibited from accessing networks containing PHI.

5.19 Good Practice 5: Guest wireless network is logged.

Hospital provides wireless network access to guests which redirects the users to a user name and password authentication page where they are granted a limited time of internet access. All user activities on the guest wireless network traffic is logged, which is a legal obligation by Turkish law number 5651[15]. The law necessitates that any organization including hotels, restaurants, malls, universities, airport, café or any other company from any industry -providing wired or wireless internet to public or to its users, for a fee or as a free service, should log the user activities going to the internet and these logs should be kept for at least 6 months. We have observed that our hospital is compliant to the law no 5651.

6. DISCUSSION

This chapter provides a comparison of laws and regulations in Turkey, EU and US; information on the current situation and network in the hospital and a suggested multilayered infrastructure based on our study.

6.1 Comparison of Regulations

Implementation of EHRs -with no doubt- helps to provide a better quality healthcare from patient's point of view. Generating a patient history record that is easily available to doctor helps to reduce medical errors. Unnecessary tests, the number and variability of treatments are reduced. Reducing the number of treatments results in cost reduction for both patients and also for healthcare organizations like social security insurance or private insurance companies so that they do not need to re-use resources for unnecessary and repeated treatments. Despite the benefits of electronic system, good quality may not be totally achieved unless its risks to security are mitigated. An important risk is the theft of medical data of a person, which is called Medical Identity Theft[16]. External parties like hackers or malicious people can obtain electronic health records by cyber-attacks to the electronic systems. The medical identity theft can also take place by insider employees. In order to protect personal privacy against medical identity theft, US has a primary law for health information privacy called HIPAA, adopted by the Department of Health and Human Services in 2003. HIPAA's Privacy Rule covers all healthcare providers including healthcare providers, hospitals, insurance companies and personal health record (PHR) vendors. HIPAA's Security Rule enforces these entities to protect EHR technically, administratively and physically[6]. HIPAA requires several standards for access control, authentication, authorization, transmission of data and notification of security breaches. Department of Health and Human Services enforces application of HIPAA standards and imposes penalties for violations. Currently when electronic records needs to be exchanged between healthcare organizations no consent from patients are required. That means patients do not have full control over their electronic health records. On contrary, individual privacy is seen as a fundamental value in EU; therefore it is addressed how privacy and electronic systems can co-exist together[16]. EU protection of health data is based on Protection of Human Rights and Fundamental Freedoms. This is very important because it enforces the healthcare organizations to record only minimally required health data, store only necessary amount of time, ensure security and provide accessibility to patient. In 2007, an EU directive specifically issued an article for Processing of Personal Data Relating to Health in Electronic Health Records and health information is defined as sensitive information that needs to be secured. It is important to note here that laws and legislation have priority over any standard. So with this clause, even without adopting or accrediting any information security standard, all healthcare organizations are enforced to ensure privacy of the citizens. With the directive, EU also defines how the EHR system should be designed, how the information will be shared between different entities and different medical staff; encryption of data, electronic authentication, control of access, backup and recovery systems, personnel policies, risk assessments for security breaches and auditing. In Turkey, although the protections against personal data are increasing they are still limited in healthcare industry. The current standard HSQS focuses on safety instead of security and privacy of patients. It has a section for information services but is limited to the service quality and does not provide a framework for information security. Opposedly however, banking industry in Turkey has very strict rules to protect customer rights. This is ensured by Turkish legislation number 5411. Banking Regulation and Supervision Agency, BRSA, (known as BDDK in Turkey) supports use of COBIT framework for the implementation of personal privacy for customers and information security for banking applications, e.g. threats against e-banking[17]. BRSA periodically audits financial institutions in Turkey and looks for conformity to the control objectives, listed as information security policies, management's support, access controls, segregation of duties, audit logs, identity management, information security and encryption, customer's consent and control over the services, business continuity and disaster recovery. Similarly, regulations in telecommunications industry protect personal privacy in a same manner; but without exemplifying with a framework. Information and Communication Technologies Authority (known as BTK in Turkey) periodically audits internet service providers and GSM operators and imposes penalties and fines in case rules for personal privacy of customers are violated [18], [19]. Regulations protecting personal health records should be improved and healthcare industry in Turkey should benefit from best practices in other industries and applications in other countries.

6.2 Current Infrastructure

Hospital has 320 healthcare staff, 7 IT engineers including their manager, 7 management personnel and 5 biomedical staff. The IT personnel are good at common IT and network management but hospital resources are not enough and employees are not specialized on healthcare application, medical device networks and network security. Our study reveals that hospital has set up its environment as a standard enterprise and has not specifically focused on information security. There is a quality specialist in the organization which is obligatory due to the JCI accreditation. However, the role is not responsible for information security. They have protection systems like firewall, IPS and antivirus which are a de facto standard for any corporate from any industry. They are receiving and implementing security updates on these systems which is observed as a good practice. However, they are not taking the necessary precautions to specifically protect personal information from insiders or against external theft. There is no data leakage prevention or no controls to detect and prevent copying of personal information to external media. Medical devices, like MRI, CT, ultrasound, monitoring systems -although support internet connections- do not connect to wireless network. Internet connections are used for external monitoring of the devices for performance when required and the necessary software upgrades by the vendors. Hospital provides smart phones to management and IT personnel; not to the healthcare staff. Mobile devices are not managed centrally and there is no control on devices like remote wipe and screen lock with a pin protection. Malicious code including worms, viruses, Trojans or spam, downloaded unintentionally by mobile phone applications or phishing mails can affect the entire network. However, it is important to note that mobile device management is almost a new concept and is not forced by regulations in Turkey yet. There is no segmentation in the network. Thus, any malicious user or a hacker who gains access to a system can easily gain access to other systems on the network. Support and maintenance personnel from vendors are granted excessive access which can pose a risk on bulk data transmission from healthcare systems to third party networks. External users should connect to the hospital network with encrypted connections and be granted based on the least privileges right. The healthcare application, -the HIS/RIS system- is a web application. As mentioned before in Section 2, web applications and HTTP are the top targets for cyber threats. Hospital can consider implementing a Web Application Firewall specialized for HTTP and HTTPS attacks. Current IPS has DDOS protection feature but there is no DOS/DDOS specialized engineers in the IT department. Hospital can consider implementing DDOS security as a managed services or as SAAS (security as a service), a cloud based security protection. Implementing cloud services brings extra controls by HIPAA standard as the traffic is being monitored outside of the hospital network[6]. However, DOS/DDOS services will hone in on the external Ethernet interfaces of the servers facing the internet in order to protect against DDOS traffic incoming to the servers from internet. So, any internal data traffic across the hospital will not be transmitted to cloud services. Although, we were unluckily not told the exact budget, management's attitude on using open-source and free tools for IT gives us a clue on their approach to security investments. IT Manager has told us that they are planning to budget % 10 percent of the total IT budget to security hardware, software and services. Top management was in the process of creating a hospital chain by establishing a new hospital in Istanbul. So, this budget is planned to be shared amongst two hospitals most of which will be transferred to the new hospital. We were told that improvements can be made most likely on the following year. The figure 6.1 is a demonstration of the current infrastructure at the hospital.

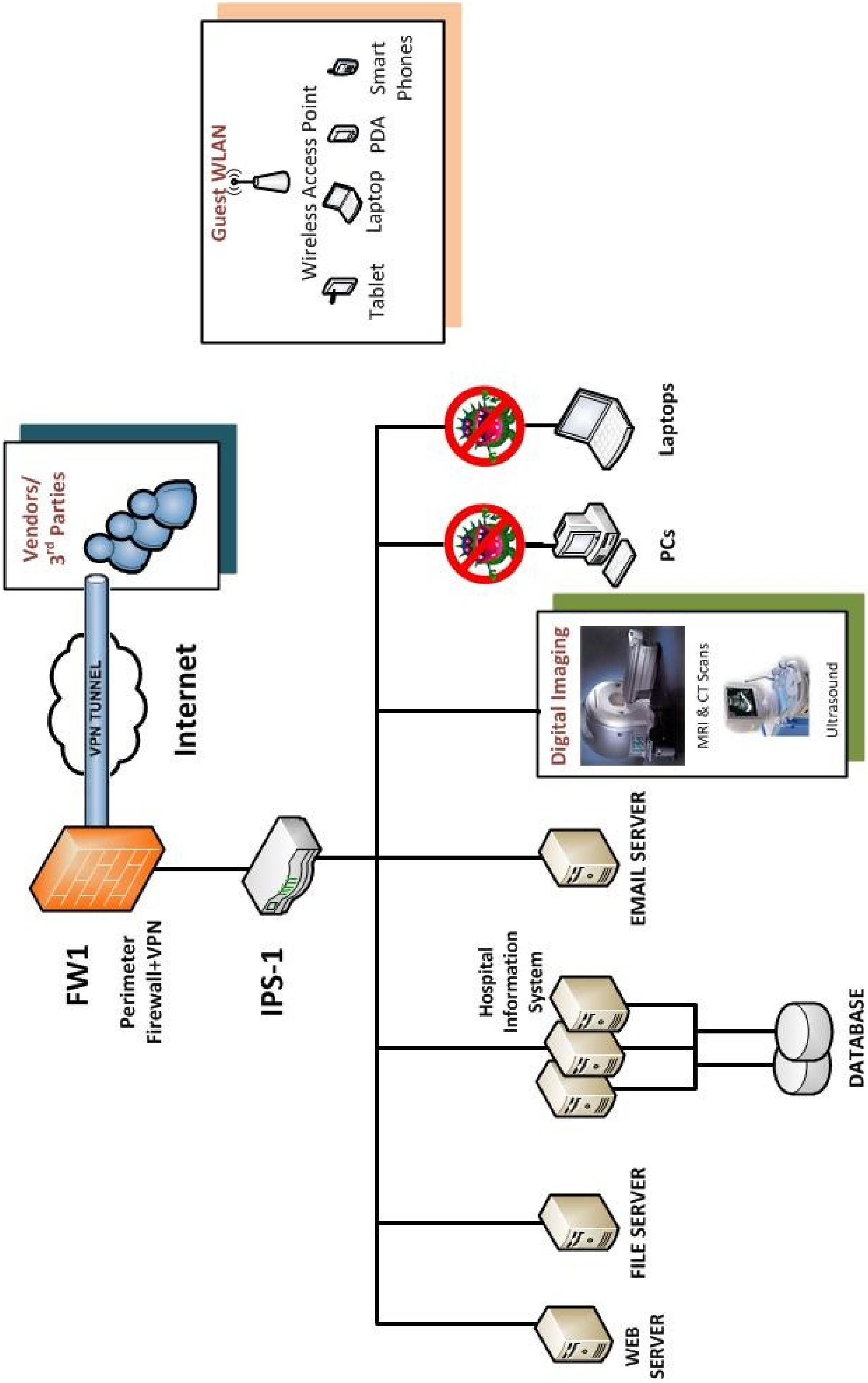

Figure 6.1 A demonstration of the current infrastructure at the hospital

6.3 Recommended Network Topology

Threats have evolved tremendously over the last decade as internet becomes an integral part of daily life. In order to protect network from all possible security breach events, the IT should understand different products and solutions, their behavior and possible vulnerabilities. Companies should adapt to new attack vectors and should be reshaped accordingly to implement security in different levels of the network[10]. The aim of layered approach is complicating a hacker's attempt by presenting different layers of security while he is trying to go through to achieve his goal; whether it is stealing data, making money or denial of service to cause reputation loss for the company. It is significant to understand the flow of data and the work processes throughout the organization while focusing on security. Just securing the firewall or antivirus is a limited approach; and it can only be an application security. In environments where many devices from different vendors are implemented, security can be insured by understanding how all the devices and work flows interact with each other. On Figure 6.2, we present network segments of a hospital which are ideally designed in different VLANs; with redundant links for each segment. Critical systems are backed up in a geographically different location. Network traffic from one segment to another is limited with authorization so only authorized users or applications can communicate within their clearance level according to the least privileges principle.

Figure 6.3 is another network topology showing the components that our hospital already has and the necessary security levels that are suggested on different segments. There is a firewall at the perimeter with VPN features, which is now a de facto for any corporation from any industry. The VPN feature allows remote users, for instance the third party companies, a secure connection for maintenance of medical devices or network components. Behind the firewall, there is an IPS at the DMZ (demilitarized zone) with DDOS protection features. This device monitors and prevents the anomaly in the network by analyzing the IP packets. The HIS server is a web application server and is already redundant. Our suggestion is to protect the web servers by a specific Web Application Server. We have suggested to use a loadbalancer in between the WAF and the web server to to ensure availability. To increase redundancy

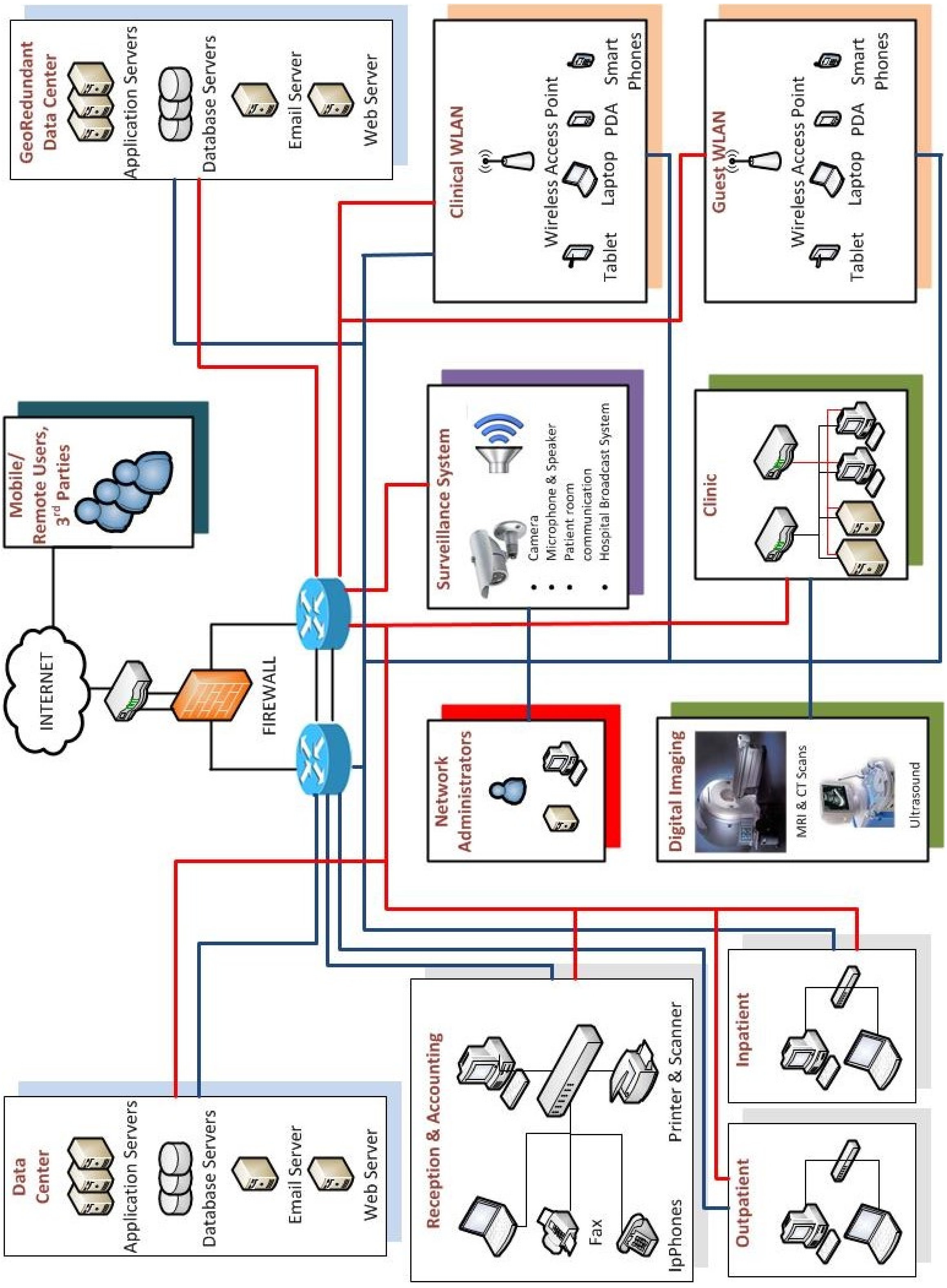

Figure 6.2 An ideal healthcare system with all departments segmented in VLANs. We recommend redundant links on each network segment with required security level. Since the management is planning to establish a second hospital, we recommend a geo-redundant data center for critical servers.

the loadbalancer as well- can be backed up with an active-passive or active-active mode device. As a suggestion, a second FW and an IPS provides another security level to the corporate network. Every computer, critical server and mobile device accessing the PHI should have antivirus. Mobile devices running healthcare related systems should have disk encryption installed. Critical files in the file servers should be stored encrypted. Databases should have encryption or masking for sensitive information. Moreover, database activities should be monitored, logged and send alerts for bad log on attempts, policy changes and administrative events. Email security should be ensured with precautions for phishing and spam mails. Email encryption can be activated where necessary to avoid sensitive information theft while sending information outside of the organization. Access and authorization should be planned correctly so that only authorized personnel access to the PHI. Access rights according to duties should be reviewed periodically so that a user should access only information that is required for a legitimate purpose; a so called principle of least privilege[20]. A logging system is suggested to collect the activities on all devices like servers, network and security devices. Any alarm on hardware or software shall be monitored remotely; both to be aware of security events or any performance issue real-time. Since the hospital management was planning to create a hospital chain by establishing a second hospital; it seems to become a large medical group soon. A future suggestion would be to have a geo-redundant system for all the critical systems for these two hospitals as many large organizations deploy. This can be a mirror system in a geographically different location to avoid data and service loss and to recover in a minimal time in case of a disastrous event like an earthquake; taking into account that Istanbul is a seismically active area.

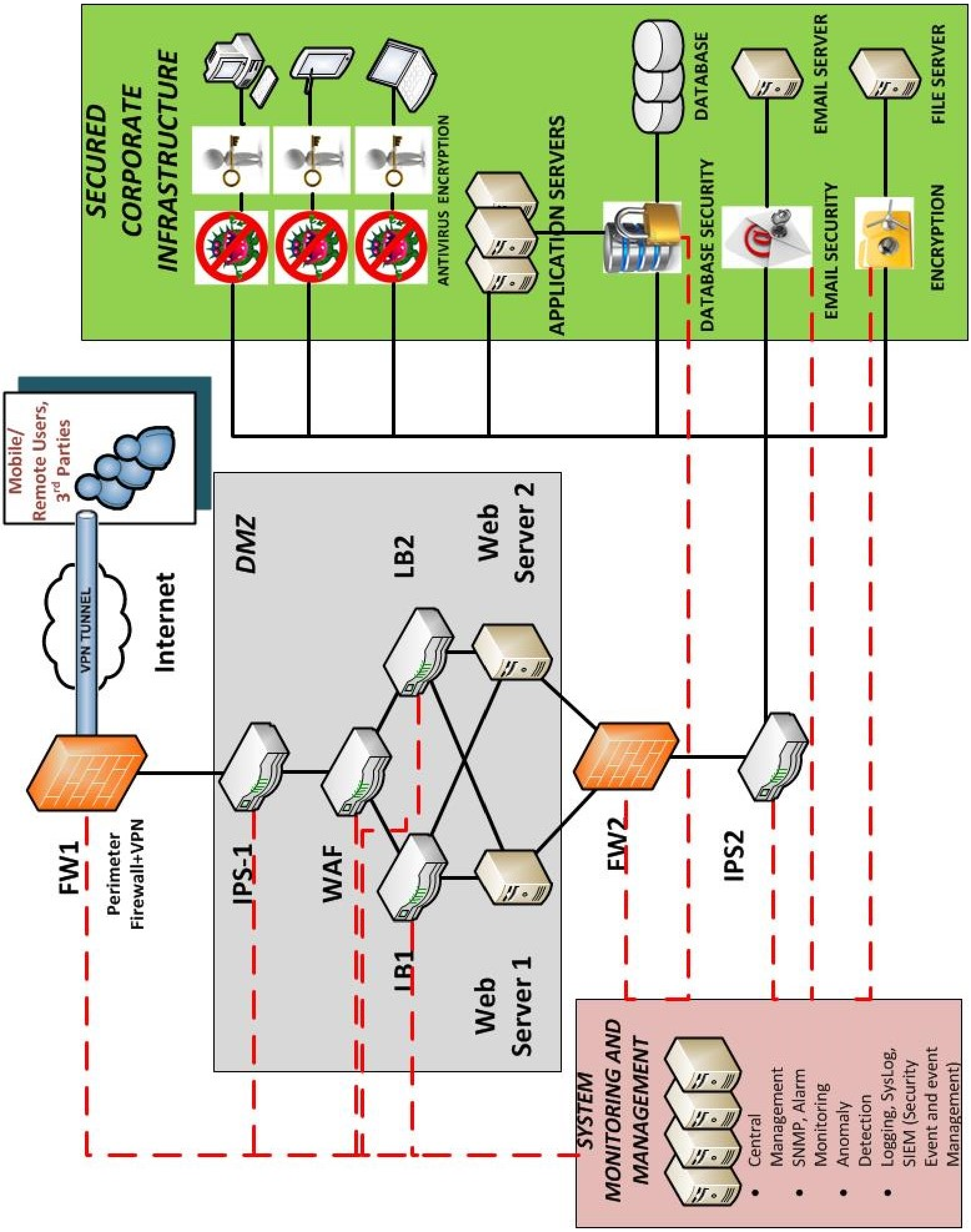

Figure 6.3 Recommended security levels. We recommend a security protection on each network layer from perimeter to endpoints.

7. CONCLUSION

In this study, we have explored how the current IT system operated satisfies the existing regulation structure; what can be done to increase the information security and recommendations for regulations in Turkey that healthcare organizations should benefit from. It is obvious that healthcare industry needs constructive and instructive regulations in Turkey. Quality is important but legal authorities should also focus on information security. The current legislation unluckily does not protect patient's privacy. Government should set sight on every single patient's security and privacy as it does on customer privacy on industries like telecommunications, electronics and especially banking. Healthcare have a lot to learn from other industries. Coming top to down, hospital management should understand the security needs of the work and support IT department in the path to patient privacy. The idea of keeping the network secure is IT department's role should change to information security is a management issue that can be solved with technical solutions. As management is involved more in security, the awareness and focus across all healthcare personnel will also increase. Coming to the IT professionals in healthcare industry, they are the decision makers for selecting the right technological solutions in practice. In today's world of complex attacks from different vectors, they should consider security in every network layer with different components on the way to protect the critical and valuable patient data and to provide a better quality healthcare with increased security.

REFERENCES

1. "Worldwide infrastructure security report," tech. rep., Arbor Networks, USA, May 2010.
2. Appari, A., and M. E. Johnson, "Information security and privacy in healthcare current state of research," *Int. J. Internet and Enterprise Management*, Vol. 6, no. 4, pp. 279–314, 2010.
3. Ashrafullah, K. M., "Information security management of healthcare system a case study of blekinge region healthcare," Master's thesis, Blekinge Institut of Technology, Ronneby, Sweden, 2010.
4. Cole, E., *Netwok Security Bible*, Indianapolis: Wiley, 2nd ed., 2009.
5. P. Campbell, B. Calvert, S. B., *Security Plus Guide to Network Security Fundamentals*, Canada: Thomson, 2003.
6. Ferrell, T., "Impact of hipaa security rules on healthcare organisations," tech. rep., SANS Institut, USA, October 2001.
7. *Application of Risk Management for IT Networks Incorporating Medical Devices Part 2–2 Guidance for The Disclosure and Communication of Medical Device Security Needs, Risks and Controls*, UK: BSI Standarts Publication, 2012.
8. Cinal, P. D. A., *Hastane Hizmet Kalite Standartlari*, Ankara: Pozitif, 2009.
9. *IT Assurance Guide Using Cobit*, IL USA: The IT Governence Institute, 2007.
10. Harris, S., *All in One CISSP Exam Guide*, New York: Mc Graw Hill, 5th ed., 2010.
11. *Application of Risk Management for IT Networks Incorporating Medical Devices Part 2–3 Guidance for Wireless Networks*, UK: BSI Standarts Publication, 2012.
12. "A risk based approach to segregation of duties," tech. rep., EYGM Limited, UK, May 2010.
13. *Information Technology Security Techniques Information Security Management Systems Requirements*, Geneva: Internation Standard Organisation, 1st ed., 2005.
14. *Critical Controls for Effective Cyber Defence*, IL USA: The IT Governence Institute, 2013.
15. *Internet Ortaminda Yapilan Yayinlarin Duzenlenmesi ve Bu Yayinlar Yoluyla Islenen Suclarla Mucadele Edilmesi Hakkinda Kanun*, Information and Communication's Technologies Authority, 2007.
16. "Privacy and security in the implementation of health information technology (electronic health records) u.s. and eu compared," *Journal of Science and Technology Law*, 201.
17. *Bankalarda Bilgi Sistemleri Yonetiminde Esas Alinacak Ilkelere Iliskin Teblig*, Banking Regulation and Supervision Agency, 2006.
18. *Elektronik Haberlesme Sektorunde Kisisel Verilerin Islenmesi ve Gizliligin Korunmasi Hakkinda Yonetmelik*, Information and Communication's Technologies Authority, 2012.
19. *Telekomunikasyon Sektorunde Kisisel Bilgilerin Islenmesi ve Gizliliginin Korunmasi Hakkinda Yonetmelik*, Information and Communication's Technologies Authority, 2006.

20. E Wallin, Y. X., “Managing information security in healthcare : A case study in region skane,” Master’s thesis, Lund University, Sweden, 2008.

21. “Coping with convergence: A road map for successfully combining medical and information technologies,” *PubMed*, Vol. 37, pp. 293–304, Oct 2008.