Informatics, Management and Technology in Healthcare
J. Mantas and A. Hasman (Eds.)
IOS Press, 2013

doi:10.3233/978-1-61499-276-9-126

Network Security Vulnerabilities and Personal Privacy Issues in Healthcare Information Systems: A case study in a private hospital in Turkey

Nihan NAMOĞLU[1] and Yekta ÜLGEN
Institute of Biomedical Engineering Department, Bogazici University, Istanbul-Turkey

Abstract. Healthcare industry has become widely dependent on information technology and internet as it moves from paper to electronic records. Healthcare Information System has to provide a high quality service to patients and a productive knowledge share between healthcare staff by means of patient data. With the internet being commonly used across hospitals, healthcare industry got its own share from cyber threats like other industries in the world. The challenge is allowing knowledge transfer to hospital staff while still ensuring compliance with security mandates. Working in collaboration with a private hospital in Turkey; this study aims to reveal the essential elements of a 21st century business continuity plan for hospitals while presenting the security vulnerabilities in the current hospital information systems and personal privacy auditing standards proposed by regulations and laws. We will survey the accreditation criteria in Turkey and counterparts in US and EU. We will also interview with medical staff in the hospital to understand the needs for personal privacy and the technical staff to perceive the technical requirements in terms of network security configuration and deployment. As hospitals are adopting electronic transactions, it should be considered a must to protect these electronic health records in terms of personal privacy aspects.

Keywords. Security, privacy, electronic health records, personal health records cyber threats, hospital information system

Introduction

In today's modern world, it is crucial to record and document, every patient's medical history, health service provided by the hospital and the recovery progress of the patient. The hospital databases are of great importance of personal payment data, social security numbers, private insurance numbers, electronic health records, diagnostic 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

[1] Corresponding Author: Nihan NAMOĞLU; e-mail address: nihan.namoglu@gmail.com

by cyber attacks and data theft [1]. The results are dramatic, because 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.

1. Information Security Risks

Recently, in Turkey, with the integration of hospital and pharmacy records with Social Security Institution, known as SGK in Turkey, personal security issues have become 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 really and only authorized personnel should have the access to these records.

Patient and payment information is exchanged between different corporates like healthcare providers and insurance companies. Moreover, hospitals, although their technical resources are skilled enough to ensure their own network operations, usually outsource to 3rd party companies that connect to hospital network for software upgrades, data backups and routine procedures for storage systems.

2. Regulatory Compliance

Data security and network security are the common Risk Management concepts for different industries like banking, insurance and telecommunication who are also dealing with sensitive customer information; therefore, the technology needs to conform to the needs of the healthcare business as well[1]. This requirement causes some processes to be redefined according to the current technological changes and it is only effective when it is supported by governmental laws and regulations in order to protect personal privacy and security.

The most common accreditation standard JCI (The Joint Commision International) audits hospitals according to safety issues that may be introduced on patients. However, it lacks the 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.

Another standard applied across public hospitals is HKS[2], announced by Ministry of Health. HKS, in contrary to JCI, includes IT regulations in consideration of patient and user security. However, it does not yet cover all healthcare organizations. HIPAA[3] in USA covers hospitals, medical device manufacturers and those who handle or transmit protected health information [2].

[2] HKS, Hastane Kalite Standartlari in Turkish translates to "Hospital Quality Standards" announced by Ministry of Health of Turkey in 2005.

[3] HIPAA, the Healthcare Information Portability and Availability Act of 1996, became law on August 21, 1996 and with it, came the promise of sweeping changes to the management and operation of security for healthcare organizations and the data they possess [2].

3. Methods

The main purpose of this project is to analyze, if the Electronic Health Records (EHR) and patient privacy are kept securely and the study will be performed in collaboration with a 150 bed private hospital in Istanbul. Initially, with a detailed study on Healthcare Standards, covering IT Risk Management like HIPAA, EN IEC 80001 and HKS in Turkey, an IT audit procedure will be generated. The hospital will be audited according to the procedure and the current assets of the hospital will be recorded and evaluated. Later, interviews will be conducted with the hospital staff, including medical personnel like doctors, nurses, technicians; the technical staff such as biomedical and IT personnel; the personnel at the information desks and managerial personnel. Finally, reports collected by interviewing and auditing will be analyzed to identify the actual shortcomings of the existing system; and, the missing but the necessary points in the current regulation criteria will be proposed.

4. Results

The expected result from this study is to reveal a general overview for patient privacy and hospital network security from healthcare personnel point of view. The outcomes from the interviews with hospital staff will show us the security awareness of the personnel, how secure the current procedures are and what their approach is to the current and future accreditation standards. Moreover; we will gather information from our security audit criteria created with the help of current regulations –like HKS applied partially in Turkey and HIPAA applied globally around USA. The challenge is ensuring the right information is passed to the right person at the right time; while maintaining Confidentiality, Integrity and Availability (CIA) of resources [3]. With this in hand, it can be possible for us to propose a report that explains the requirements that needs to be added to the auditing standards that should be common across the country.

5. Discussion

In order to maximize productivity, it is essential to simplify the user experience on the EHR and the personnel should be updated with regular trainings on user and patient security and privacy. To cope with the excessive amount of data in healthcare systems and the evolving threats that are motivated to reach this mass of data, can only be achieved through collaboration of health and technical professionals in government and healthcare business. More realistic outcomes will be discussed when the study comes to an end.

References

[1] A. Appari, and E. Johnson, Information security and privacy in healthcare:current state of research, *Int. J. Internet and Enterprise Management Vol.* **6** (2010) *No. 4*, 279–314.
[2] T. Ferrell, Impact of HIPAA Security Rules on Healthcare Organizations, SANS Institute, 2001
[3] E.Wallin, Y. Xu, *Managing Information Security in Healthcare: A Case Study in Region Skane*, Lund University, Sweden, 2008