Threats and Challenges to Security of Electronic Health Records

Shalini Bhartiya[1] and Deepti Mehrotra[2]

[1] IITM (GGSIPU), New Delhi, India
[2] ASCS, NOIDA, India
shalinibhartiya69@gmail.com, dmehrotra@amity.edu

Abstract. Healthcare has always been a sensitive and a complex process. Rapid strides have been made both in the field of information technology as well as health care successfully integrating both for better facilities and services offered by the health-givers. Electronic health records (EHRs) is the product of this integration and forms an integral part of the automated healthcare system. Accessing of EHR by each stakeholder complements the issues of data disclosure, confidentiality, authenticity and privacy that are likely to occur due to many reasons. This paper aims at studying and identifying security threats to EHR in the hospital information system currently prevailing in the hospitals (HIS). It further categorizes the threats based on security characteristics and rates them on the basis of impact and magnitude of loss to the patients. The paper highlights real-time scenarios with each as an important requirement of the health-givers on one hand, can also be a reason of security breaches on other hand. It concludes by listing challenges and recommendations to curb security threats commonly found in the physical setup of healthcare environment.

Keywords: Challenges to EHR, EHR, HIS, Security, Threats.

1 Introduction

The health industry is undergoing a fast transition from its conventional method of care-giving. E-health or Health Informatics is an ICT-integrated method adopted by the hospitals for providing healthcare services to the patients anytime, anywhere without any restriction of location or facility. Hospital Information System (HIS) is a customized and tailor-made application facilitating the care-providers requirements through integration of components from IT as well as medical domain. HIS accumulates entire details of patient's health in form of electronic health record (EHR).

HIS includes various processes including registration, billing, admission, prescription, investigation registration and reports, discharge summary, appointments, medico-legal requirements, to list a few. Each process is handled individually by well-organized schemas called departments in the hospital that are constantly communicating and sharing the health information for delivering the facilities to the patient. The transfer of health information between departments electronically, opens a new door for theft and disclosure of sensitive and confidential data to unauthorized and unidentified users.

K. Singh, A.K. Awasthi, and R. Mishra (Eds.): QSHINE 2013, LNICST 115, pp. 543–559, 2013.

Though data is crucial for the productivity of any business, the varsity of ensuring confidentiality and privacy of health data outcasts other industry needs.

Confidentiality is a form of informational privacy characteristic of certain relationships, such as the physician-patient relationship. Personal information obtained in the course of that relationship should not be revealed to others unless the patient is made aware of this intention and consents to disclosure [9].With all the security systems like firewalls, Intrusion Detection Systems (IDS), anti-virus software, encryption/decryption techniques and role-based access grants, there is enough room for security exploits to EHR. Currently deployed hospital information systems reveals many grey areas that accumulate to security threats and data breach or disclosure of health data and largely by the insiders.

The prime objective—'providing health care to the patients' directs the users to surpass the security rules imposed in the application. Here, in this paper, we have discussed the scenarios where the confidentiality and privacy of EHR is deliberately compromised. We are strictly limiting the discussion to security aspect of storage and retrieval of health data by the care-providers i.e. doctors and paramedical staff and also the patient.

This paper is divided into nine sections. Section I is an introduction to Health Information System (HIS) and the security concern of electronic health records in electronic setup. Section II reviews the work done by other researchers to gain better insight of security issues in health informatics. Section III details the research methodology used to collect and analyze the findings related to current practices and security threats in the real working environment of the hospital. Section IV tabulates the conveniences and constraints of health informatics as described by clinicians. Section V enlists the varied security threats and probable reasons of their occurrence and Section VI elaborates the real-time scenarios that require concentration and focus to develop more specific and suitable security solutions. Section VII pens down the possibilities of stress and challenges while accessing EHRs. Section VIII states the suggestions to overcome the challenges to security of EHRs in various scenarios. Finally, Section IX wraps up emphasizing the importance of health informatics and the need to develop suitable security solutions in this area.

2 Literature Review

The integrity, availability and confidentiality [7] of digitized health data becomes the highest priority for developers as well as end-users. Profound study on the security aspects of electronic health records (EHR) world-wide, significantly states the demand and acceptance [1] by the healthcare industry in transforming its services into digital-based environment. The confidentiality and privacy of sensitive health data of patients moves out from the physical lock and key security to uniform and standardized bits and bytes structure. EHRs do deliver greater mobility and accessibility to information [11], but can also increase security risks if the appropriate precautions are not taken. Unlike paper records, access to EHRs can be restricted, so staffs have access to records based on job function. Specific to protecting the information stored in EHRs, the HIPAA [6] Security Rule requires that health care providers set up physical, administrative, and technical safeguards to protect electronic health information. NIST [14] has developed guidelines to facilitate application of appropriate levels of information security according to kind of impact or consequences that might result from the unauthorized disclosure, modification, or use of the information or information system. The guidelines are based on review of categorization of security terms and definitions by FIPS 199. World Health Organization [12] has given guidelines about how to review the current health record systems before discussing issues and challenges to the security of EHR. As emphasized by [2], protecting the health information from unauthorized access and malicious attacks would enhance confidence and acceptance among its stakeholders. Effort is required as stated by [5] to incorporate compliance like HIPAA security guidance with own security policies in standardization of HIS at the national and international level.

The table highlights the findings of few surveys [13][15][16] conducted with an objective of identifying security issues and solutions adopted by security managers in healthcare and other industries.

Table 1. Review of Surveys conducted on Security Issues in Healthcare

Survey	Objective	Finding
CSI3 Computer Crime and Security Survey 2009	To identify the areas of data theft and breaches in various industrial setups including healthcare	60% of total financial losses resulted from "malicious insider" attacks
2011 HIMSS Security Survey, November 2011	To identify key issues surrounding the tools and policies in place to secure electronic patient data at these healthcare organizations. An important component explored in this study is the issue of risk analysis.	Three-quarter of healthcare organizations are doing risk assessment and using it to determine which security controls should be put into place. Survey revealed that there is no robust plan for securely sharing the information outside of their organizations.
CSI Computer Crime and Security Survey, 2010-2011. Survey included security Practitioners from various sectors	To determine not only what security technologies respondents used, but additionally how satisfied they are with those technologies.	Malware attacks are the most commonly seen attack. Managers are looking security solutions in virtualization, cloud computing and exploring better visibility into security status of the networks
SearchHealthIT.com, April 2011	Are hospitals meeting federal laws like HIPPA for data protection and what security policies and measures they think to implement in near future for security of healthcare data	The respondents focused on encryption and tighter access controls for HIPPA privacy compliance in networked environment. Single sign-on (SSO) is also being acknowledged as a strong authentication method in integrated EHR system

The security issues perceived by an IT manager and hospital manager do not fall in the same domain of thoughts. In addition to the security characteristics[3] as prominently talked about in Information Technology, security principles in healthcare environment include the ethics, right to information, legal rights, laws and legal implication for both—care-provider and the patient. Integration of ICT and healthcare faces tough challenges associated with its adoption especially in developing countries as illustrated by [5] taking the example of Tanzania. The conditions can be evidently analyzed in Indian perspective [8] due to the similar financial, educational and social conditions. The cross case effect matrix generated by [4] identifies the basic functionalities and its effects on security of health records. The Department of Information Technology (DIT) and Ministry of Communication & Information Technology (MCIT) have prepared a framework [10] for Information Technology Infrastructure for Health (ITIH) in India with the support of Apollo Health Street Limited (AHSL) to build a secured and robust digitized healthcare environment. Framing of strong privacy law, legal regulations, policies and acceptance of digital records as legal evidences in the court can foster an optimistic absorption by healthcare professionals.

3 Research Methodology

It is a questionnaire based study conducted at public sector, government controlled chain of hospitals under labour ministry. There are about 2026 integrated sites through centralized data center controlled by IT vendor and its team. The study was made at one of these centers to observe the usage of application and gather the opinion of clinicians and paramedical staff with an objective of identifying the security applied to health records and also where the data is vulnerable to security threats and breaches. The study covered all the areas of services i.e. OPDs, IPDs, Day-care, Casualty, OTs, ICUs and IT control room, Laboratories and Pharmacies. Stratified sampling method was used to collect the views selecting Professors, Associate Professors, Senior/Junior Residents and Interns from each department. Besides, other prime clinicians were approached that include nodal officers, operational heads, medical superintendents, recruitment heads, anesthetists etc. The feedback of 200 clinicians was collected through well-structured questionnaire distributed to the clinicians. The questionnaire focused on questions related with data availability, entry-points in the system and possible vulnerabilities, authentication controls, ease of use, increase in efficiency of health-providers, etc. One set of questionnaire was also uploaded on Surveymonkey.com for the purpose. Besides questionnaire, informal interviews and meetings were used to gather relevant information.

4 Clinician's Perspective

The clinicians acknowledged the long and short-term benefits of having E-health Records. They strongly agree that electronic health data can substantially reduce the risk of data breach but found the recording methods and interfaces as time-consuming, inappropriate and substandard. As an instance, a senior doctor selects a team of junior doctors for treating or operating a patient on case-basis, requiring sharable access of case-sheet to all the members of his/her team. The team might remain same or have modifications depending on case-to-case. This results in a multiplicative distribution of rights and privileges to the doctors as well as paramedical staff that they continuously hold even after the case is closed. Here, we present clinicians views based on their hands-on experiences of using HIS. Their conveniences and constraints with respect to usability, availability and security of EHR are represented in tabular form below.

Table 2. Clinician's Conveniences and Constraints in using Hospital Information Systems for storing and accessing EHRs

FEATURES	CONVENIENCES	CONSTRAINTS
Password-Based or Role–based Access to Data	➢ Guarantee access to only legal users ➢ Enhances trust and belief in the system ➢ Helps department heads in tracking and analyzing efficiency and errors on individual basis	➢ OPDs are handled by team of doctors, sharing the same computer disallowing simultaneous update of records in the database. ➢ Doctors on adhoc appointments do not have separate login Ids and are forced to share the Ids of their colleagues or HODs. ➢ Cannot control the disclosure of information between doctors
Ease of Use	➢ Patient details are readily available ➢ Easy maintenance of health details and reports	➢ Requires use of multiple keys and opening of various windows, increasing the effort and time of data-entry ➢ The interfaces are not satisfactory ➢ Takes a lot of time to retrieve data ➢ Improper training takes more time to understand the working of HIS
Efficiency	➢ Enables correlation with previous history and observations ➢ Past records and history of patient helps in better diagnosis	➢ Cannot be used during heavy flow of patients mainly in OPD. ➢ Criticalities like Casualties and Emergencies cannot be dealt with the HIS alone. ➢ Time consuming data entry methods ➢ Slow processing adds to delay in work

Table 2. (*Continued*)

FEATURES	CONVENIENCES	CONSTRAINTS
IT Skills and Knowledge	➢ Enables independently handling of processes and various devices like scanner, printer etc.	➢ Requires practice and training to gain better grasp on the usage of the system ➢ Recognizable constraint among doctors in the age group of 50 and above. ➢ Need the help of trusted colleagues or paramedical staff to record entries
Availability of Data	➢ Investigation and Prescription details are available in respective departments. ➢ Record can be accesses from any location ➢ Health Data of a patient can be accessed from anywhere without any location constraint.	➢ Complete details of the patient is not always available ➢ Referral patient's data is not available ➢ Investigations done outside the hospital are never recorded. ➢ Typographical errors and data mismatch needs manual verification
Security	➢ Cannot access the application without valid login Ids and passwords ➢ Access to only relevant processes ➢ Restricted and Controlled Internet usage. ➢ Suppress all e-mail services except for intranet mail-box.	➢ Uncontrolled printing of documents and reports. No logs available to identify the number of prints taken for any record. ➢ No control and track on patient's information is being sent outside the hospital. ➢ Sharing of computer or records hides the individual identity of the user. ➢ No monitoring and restrictions on modification of health data.

The figure illustrates the conveniences and constraints of the doctors using the HIS for providing healthcare services. Relative frequency percentage was calculated for each parameter and enabled to identify usability, availability and Security of health data along with improving efficiency and requiring IT skills for using the application. It was observed that 21% of respondents found password-based access as satisfactory. 20% found acquiring skills to use the application as an overhead explaining that the prime objective is providing healthcare to the patients.

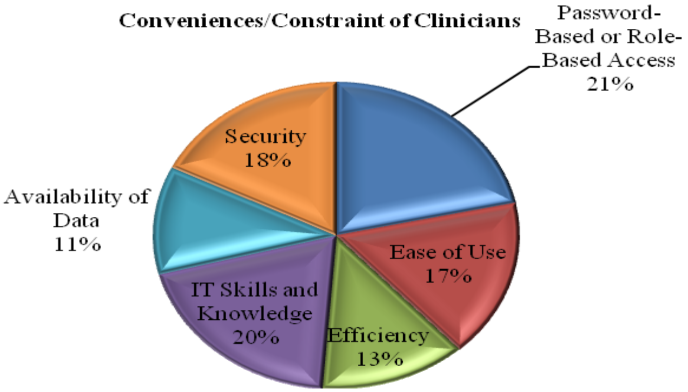

Fig. 1. Shows the relative frequency of clinician's experiences of using HIS

5 Prevalent Security Threats

As technology continues to play an increasingly important role in health care, the national movement towards electronic health record systems is leading to many improvements in the quality of patient care. Yet, as with paper record systems, there are risks. Healthcare Information systems (HIS) are exposed to numerous threats that can result in significant loss and damage to medical records. The survey identified numerous confidentiality and privacy vulnerabilities prevalent in the system with some due to ignorance of its stakeholders and others due to the current practices of healthcare.

Password Sharing: Password sharing poses threat to data integrity and repudiation of EHR. Data confidentiality and privacy is at stake as the study showed that more than 80% clinicians share their passwords with fellow colleagues.

Typographical Errors: This is a threat to accuracy and correctness of EHRs. Healthcare industry is highly error-conscious and accuracy is of prime concern here. Typographical errors are common threat mainly due to lack of technical skills found in data-entry operators.

Physical Security: Unauthorized penetration into the hospital vicinity is an additional physical threat to the availability and security hospital infrastructure including devices, equipments and medical records. Inappropriate and insufficient of physical security exposes health data to illegal and unauthorized disclosure and malfunctioning.

Storage of Backups: Storage of the backups is more crucial that taking backup. The security of stored data, especially backup data, has received less attention. A policybased multi-backup data on a regular schedule, storage of backups off site at multiple locations and ensuring that backup media is physically secured needs to be ascertained to protect the sensitive health records.

Timely-Availability of Data: The non-availability of health records during system upgrades or power failure is not accepted by the clinicians. The healthcare needs cannot afford any downtime whatever minimum it may be.

Role-Based Access: Users in health informatics system get to access only relevant details as per their working profile in the hospital but changes to default access roles are frequently demanded due to shifting duties mostly by paramedical staff. The privileges once granted are never reverted.

Threat from Former Employees: The active IDs of former employees are another threat that provides the opportunity to disgruntled or terminated employees to perpetrate into the system. Restraining orders, password changes, and other special security measures are necessary in some situations.

Table 3. Frequency of Common Security Threats to EHRs as observed in working environment of health care

THREATS	FREQUENCY	PERCENTAGE
Sharing Passwords	177	89
Typographical Errors	104	52
Physical Security	151	76
Storage of Backups	77	39
Timely-Availability	126	63
Deficiencies in Role-Based Access Controls	138	69
Former Employees	81	41
Personal Details of Patients	179	90
Password Policies	185	93
IT Privileges	140	70

Personal Demographics of Patients-A patient becomes a victim of identity theft because his/her demographic or personal details are accessible and modifiable from any workstation.

Password Policies-Authentication through valid login Ids and passwords is the most common choice of any IT administrator. To strengthen the authentication controls, health informatics must incorporate robust password policies that demand changing of passwords periodically and encourage users to choose strong passwords.

IT Privileges-IT people hold absolute rights and privileges to manage and control the processes of health informatics. The clinicians viewed it as a threat to confidentiality and privacy to health data.

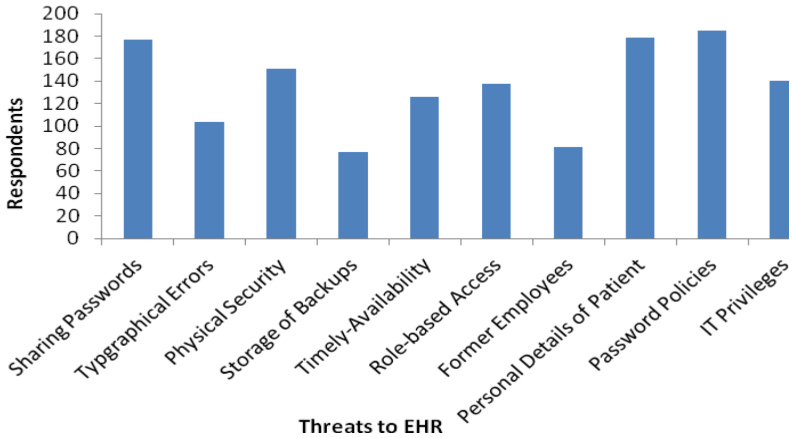

Fig. 2. Frequency of Security threats and Vulnerabilities to health data as perceived by the Clinicians

Table 3 lists the frequencies of security threats as perceived by the clinicians. Figure 2 graphically represents the clinician's perception about each of the threats exposing data to numerous security breaches in healthcare environment. The impact of weak password policies, exposed demographic details of the patient and sharing of passwords is high whereas typographical mistakes, security of storage of backups and former employees are considered as having low impact on the security of health records.

Other Factors

Training and Education—Lacking

Hospital management arranges and schedule training module for their employees once a while but it is not a continuous process. The staff demands more adequate training and hands on practice sessions to be conducted to be able to efficiently operate the HIS. Observations found the staff comfortable using their regular part of the modules or activities but lacked knowledge to operate other parts also under their control.

Compliance

Standards like HIPAA, HL7, and DICOM were either not known to majority of the staff people in the hospital or was not given much weight age and consideration for the compulsory inclusion of these standards in the system. Patients usually have no or restricted access to their health information where they can view their investigation reports and test details or book an appointment with the doctor prior coming to the hospital. The patient has no access to complete diagnostic and history of his/her case.

Patients are not aware of their rights regarding the authority of their health records and obligations of the hospital relating to storing and securing their confidential health information.

Security in Place

Role based access privileges are given to each user and the department according to their requirements. Firewalls with full scan and Proxy servers are installed to monitor and record all the network traffic. The internet access is available to only few privilege users of the hospitals like HODs, MS, Additional MS, and Nodal Officers. Other health-providers requiring internet access is given controlled and restricted access completely monitored and recorded. Logs of each transaction are maintained along with the details of the employee logged in at that point of time. Every transaction made by the user is directly recorded at the centralized data-centre. Patches and updates are incorporated whenever required. The system works in closed network where no outside access is provided to the users. The system incorporates a private mailing process whose use is restricted to high profile users only or some paramedical staff members. Multiple servers supporting every operating system are installed. Hardware Firewall and proxy servers are installed enabling security checks at each network points for any type of data communications and transmissions.

6 Current Practices

Health information is characterized by high complexity and heterogeneity in both the nature and the sensitivity levels of the different data sets included in it. Sensitive health information such as HIV status, obstetrics history and mental health history could become more easily accessible as health records become fully automated. If sensitive health information is accessible by others, this would clearly represent a breach of the patient's privacy.

Security is generally defined as the extent to which personal information can be stored and transmitted in such a manner that access to the information is limited to authorized parties. The threats described in the previous section are very common, found in any business environment. But the slightest possibility of their occurrence in health industry can cause a high magnitude of loss to exclusively patients and also the hospital. The question arises-"What forces the clinicians to compromise the security of EHRs in health informatics system? "

The answer lies in the current practices of care-giving. The weak integration and communication between departments exposes patient's identity and health data forfeiting security mechanisms and policies altogether. A deep thought and attention needs to be given to the following scenarios that justifies that abiding by the security rules and policies are out of control of doctors and hospital administrators.

Real-Time Scenarios

E-health security and privacy are challenging not only due to the difficulties of developing an error-free, complex framework, but also because of the complications of various issues addressed by all the stakeholders in the E-health industry such as the patients, vendors, and health providers.

Our observation identified that clinicians want to follow procedures of HIS but various limitations and demands of the environment of health care forces them to compromise with the confidentiality and privacy of EHR. Here, we present a few of real-time scenarios that act as a barrier to security of electronic health data of the patients.

- ➢ Frequent shift of duties and departments is very common among the doctors and paramedical staff. This forces the IT admin to modify the default access control lists (ACLs) as per the demands of a particular facility and services. The ACLs once modified remain in that state till the administrator receives requests from hospital-in-charge.
- ➢ Hospital Laboratories are not fully equipped to cater to every need of the patient. Hence, many tests are outsourced exposing the patient's sensitive health data to outside world.
- ➢ Investigation devices are not programmed to transfer images and findings to the health informatics system. The diagnostic details have to be typed either by the clinicians or support staff thereby surpassing non-repudiation and authentication controls.
- ➢ OPDs have a heavy flow of patient's every day. The HIS take about 5 to 10 minutes to view, add and update each patient's information. It becomes impossible to manage the waiting queue outside the doctor's room. Moreover, the systems are slow and hang up quite frequently.
- ➢ The wards and rooms do not have computers at the bed-side of patient, except for in ICUs. Moreover, the doctors on round can't afford the time taken to display the progress of each patient by HIS.
- ➢ The hospital administration policies permit the staff to take prints of confidential and health related documents any number of times. No written entries were found in the logs that could identify the number of print-outs taken by an employee at any given point of time.
- ➢ Emergencies and Accidental cases require immediate action. The doctor-on-duty has to provide the utmost care and treatment to the injured. Such details sometimes are never recorded due to non-availability of electronic details of the concerned patient or are forgotten over the period of time to be recorded into the system.

Impact of Real Time Scenarios on Security of EHR

Breach to EHR causes devastating damage to the healthcare industry's reputation and is a serious detriment to the goal of building a patient-centric paperless model to be used by the care-providers without any limitations or constraints. Here, we categorize the activities and services as observed in the current practices into type of security threat and further classify the impact of that threat on the security of EHR.

Table 4. Impact of Current Practices on Security Features in Health Informatics

Scenarios	Security Threat	Severity
Frequent Shift of Duties	Data Disclosure	Low
Outsourcing of Investigations	Confidentiality Loss	High
Handling Emergency and Accidental Cases	Data Integrity Loss	Medium
Non-Integration between Medical equipments and HIS	Data Availability	Medium
Reluctance of Doctors	Data Integrity Loss	High
Handling OPDs	Data Integrity Loss	High
Resource Sharing	Non-Repudiation	Medium
Ignorance of Patients	Identity and Confidentiality Loss	High

Table 4 shows the type of security threat and its severity level in each of the scenarios rampant in health informatics. The analysis brings out two important features that need to be prioritized while planning and designing any HIS. The reluctance of doctors and outsourcing of investigations are ranked with high level of severity. Reluctance is a mindset which can be changed with user-friendly interfaces and training. Outsourcing of investigations cannot be eliminated as no hospital can be 100% equipped with all the machines and devices required for varied laboratory tests, therefore, needs automatic integration with the hospital information system. Thus, as much organized the application is, without a rigorous security plan, the main objective of developing E-healthcare environment would forfeit.

7 Challenges to EHR

The logics behind the accessibility of data, as observed during the survey, were found to reflect a static behavior i.e. the rules and policies uniformly applied to every component and process of HIS. To be effective, security must be multi-layered and if it fails, measures must be in place to safeguard the health data from access.

Here, we address certain issues that openly challenge the security and usability of health informatics system.

Interoperability

Interoperability addresses issues of how to best facilitate the coding, transmission and use of meaning across seamless health services, between providers and patients. Its geographic scope ranges from local interoperability (within, e.g., hospitals or hospital networks) to regional, national and cross-border interoperability. It is required across heterogeneous EHR systems in order to gain the benefits of computerized support for decision making, workflow management and evidence based healthcare. The information captured in EHR systems provides easily retrievable data via networks and creates significant risks representing unique security challenges.

Data Availability

With little and inadequate medical knowledge, patients can misinterpret the investigation results and diagnosis. Entire information available on internet gives rise to cyberchondria, i.e. self-diagnosis by the patient without consulting the physician. The doctor might find it difficult to satisfy the patient's queries when every technical term is exposed to the patient. It might result in doctor going into restless or indifferent state due to panic and disturbances created by the patient. The display of entire health reports can cause mental and social trauma to the patient as every person has a different level of handling stress. This can result in image defamation, loss of job, emotional distress, family neglect, social stigma blocking every path to recovery.

Data Confidentiality and Privacy

The EHR is vulnerable to threats from various secondary stakeholders of the system as identified during the survey. Every single unit of data passes through networks established and controlled by the IT team giving them implicit privileges to peep into the confidential and sensitive health information of the patients. The health data accessed by the employers as per the policies of the organization can be used against the benefits of the employee. Insurance companies can deny claims and benefits to the insurer. The friends and family of the patient can easily access the investigation and other details even without his/her consent.

Internet

Internet is a source that binds the world in a close-knitted family where everyone can interact and share their thoughts and intelligence. Doctors believe that internet is a useful resource of sharing health data with the desired stakeholders. It would result in reduction of cost and time in making the information available to the people. It enables location-independent facility of not only availability of health data but also rendering of services by doctors. E-mail is one such facility that enables communication and transfer of important documents between the two parties. A typographical mistake in sender's address can deliver the reports to unintended person. E-mail spoofing is another threat and a challenge to security of EHR. Bulk-mail can result in non-delivery of some mails that are never checked or send again unless being explicitly demanded by the patient. Patients never bother to update E-mail accounts when changed, with the hospital. Not all patients have their own E-mail Ids or Internet access. Uncontrolled and unmonitored dependency on service providers for E-mail services questions the reliability and security of EHR.

Policies and Standards

How can a doctor take the consent of a patient in unconscious state before treating him/her? This is an important question that challenges the HIPAA rule of taking patient's consent before accessing his/her medical records. Moreover, if we talk about in Indian perspective, as per the Census of India's 2011, of the 121 crore Indians, 83.3

crore (68.84%) live in rural areas that still lack technological resources. Similar diversities can be acknowledged in other parts of the globe. Hence, the standards like HIPAA, DICOM needs to be restructured to reflect and accommodate these diversities. Security of EHR is challenged due to lack of uniform, multipurpose data standards that meet the needs of the diverse groups who record and use health information. There is a lack of policies and legislations to protect privacy while permitting critical analytic uses of health data. Serious intervention of government is required in formulating policies and laws for health informatics.

IT Team

The IT team enjoys full rights and privileges on every resource and data of the health informatics system. Configuration errors might lead to hacking or other attacks on health data. Ignorance of IT companies while developing HIS is a major challenge that drags users away from using the HIS.

8 Recommendations

The study and analysis discussed above reflect the security threats and challenges prevailing in a closed network of health departments in hospitals that are located in different cities. Threats to confidentiality and privacy of data are more from insiders in such an environment as the outsiders have negligible and controlled role to access these records. The stakeholders demand an efficient system that could enable the availability of accurate health record information that is truly integrated with all the databases. The system should be able to recognize the user on per-transaction basis that can be held accountable for the acts committed by him/her if any discrepancy or inconsistency is observed. The security controls and models require refinement where the following factors should also be taken into consideration:

- A vigorous plan for physical security of the hospitals units and departments especially at night would reduce the possibilities of theft of physical devices and documents.
- Providing controlled and limited powers and privileges to IT vendors responsible for developing and maintaining the hospital management systems and its databases.
- Developing and implementing dynamic access controls that could allocate and monitor the authorization of each stakeholder from time to time or as per the demand and need.
- An inbuilt or implicit check should be imposed on various internal processes of the application, such as, keeping a count of printouts taken, use of external storage devices, use of internal commands and shortcuts, accessing the records of deceased patients etc.
- Primary users of healthcare are doctors. The system generally allocates identical authorization privileges considering them at the same hierarchy. The authorization and access controls should be assigned based on qualification, experience, designation of the doctor on one hand and the

justified request on the other hand. The request can be justified by supporting the application with decision-support system that can intelligently view and analyze the request based on the attributes provided in the query.

- Security controls complemented with accountability ensures better trust and confidence among stakeholders of the system. Hence, measures and policies must be designed and framed that would strengthen non-repudiation in sharable and interoperable healthcare environment.
- The role of a doctor as well as paramedical staff administer frequent shift of duties in their everyday working. The RBACs needs to be frequently altered to accommodate their data needs. Therefore, strict actions are required that could dynamically allocate and also de-allocate the privileges and permissions on various areas of the application, probably bounded by a time-frame.
- There is huge diversification of location, education, population, funds and resources not only around the globe but also within the nation. It is required to design standards like HIPAA, HITECH Act, HL7 and DICOM around these parameters so that security controls on EHRs can be imposed irrespective of the heterogeneity and interoperability of health data stored in such diversified environments.

9 Conclusion

The study revealed many facts related to the usability, availability and security of electronic health records accessed by the care-providers in their daily practices. The hospitals are well equipped with full-fledged HIS but most of the clinicians were found reluctant to use it in their daily practices due to various reasons. Due to low and partial usability, the transformation of health records to electronic form still remains incomplete and the hospitals maintain and use the paper-based records in parallel with the EHRs. Huge rush of patients in OPDs every day (Average: 2000 patients), it is difficult to manage and provide healthcare services totally depending on the HIS. The system generally slows down at such times resulting in non-availability of patient’s information during treatment. Additionally, the IPDs have computers placed only at the nurse’s workstation, forcing the doctors to refer to case-sheets while taking rounds in the wards and rooms of the patients. The frequent shift of duties of paramedical staff forces the IT manager to assign added privileges for them, exposing the sensitive patient’s data to a larger hierarchy of users.

Security, integrity and privacy of personal medical data is of utmost importance, and whilst many research projects worldwide are investigating the application of new technologies to E-healthcare solutions, security and reliability of these technologies is an area that requires further exploration. This paper highlights security threats and their impact on the day-to-day working of health care environment in a closed network. The collection and analysis of health information demonstrated real-time scenarios that require deep and futuristically planned security mechanism or a model capable enough to enhance the confidence and trust of physicians on health informatics. The health care systems are relatively to protective measures to keep the security and privacy of their patients and their health details. Business process redesign and an understanding of the change management process are fundamental to this activity. Healthcare organizations need to analyze and assess usages of EHRs with different perspectives and reflect such perceptions in proposals, system selection, development, installation, and implementation of health informatics system in order to ensure that all needs of the organization are met.

References

1. Fisher, S.R., Creusat, J.-P., McNamara, D.A.: 2008 McKesson Corporation, Improving Physician Adoption of CPOE Systems, http://www.strategiestoperform.com/volume3_issue2/docs/ImprovingPhysicianAdoption.pdf
2. Lin, S.-C., Tsai, W.-H., Tseng, S.-S., Tzeng, W.-G., Yuan, S.-M.: A framework of high confidence e-healthcare information system. In: International Conference WWW/Internet 2003 (2003)
3. Alanazi, H.O., Jalab, H.A., Alam, G.M., Zaidan, B.B., Zaidan, A.A.: Security characteristics: Securing electronic medical records transmissions over unsecured communications: An overview for better medical governance. Journal of Medicinal Plants Research 4(19), 2059–2074 (2010)
4. Fernando, J.: Jabberwocky, The Nonsense of Clinician Ehealth Security. International Journal of Digital Society (IJDS) 1(3) (September 2010)
5. Omary, Z., Lupiana, D., Mtenzi, F., Wu, B.: School of Computing, Dublin Institute of Technology, Tanzania Case, Analysis of the Challenges Affecting E-healthcare Adoption in Developing Countries: A Case of Tanzania. International Journal of Information Studies 2(1) (2010)
6. HIPAA Compliance Review Analysis and Summary of Results, Centers for Medicare & Medicaid Services (CMS) Office of E-Health Standards and Services (OESS), Reviews, 2008 HIPAA Compliance Reviews CMS Office of E-Health Standards and Services (2008)
7. Appari, A., Johnson, M.E.: Information Security and Privacy in Healthcare: Current State of Research (August 2008)
8. Patients' and Citizens Task Force of the European Health Telematics Association (EHTEL), Angelica Frithiof, Rod Mitchell, IAPO, Nicola Bedlington, European Patients Forum, Harm Jan Roelants, Jean Luc Bernard, Le CISS, Johan Hjertqvist, David Garwood, Formulation of policies and standards: The Electronic Health Record, A Position Paper, 25 September (2006)
9. Gostin, L.O., Turek-Brezina, J., Powers, M., Kozloff, R., Faden, R., Steinauer, D.D.: Privacy and security of personal information in a new health care system. The Journal of the American Medical Association 270(20), 2487–2493 (1993)
10. The Department of Information Technology (DIT) (Ministry of Communication & Information Technology (MCIT)) with the support of the project Implementation Agency Apollo Health Street Limited (AHSL), Framework for Information Technology Infrastructure for Health, vol. I, II (2004)

11. Wainer, J., Campos, C.J.R., Salinas, M.D.U., Sigulem, D.: Security Requirements for a Lifelong Electronic Health Record System: An Opinion. Open Med. Inform. Journal 2, 160–165 (2008)
12. Electronic Health Records: Manual for Developing Countries, © World Health Organization (2006)
13. 2011 HIMSS Security Survey, © 2011 Healthcare Information and Management Systems Society, supported by The Medical Group Management Association (MGMA) (November 2011), http://www.himss.org
14. Guide for Mapping Types of Information and Information Systems to Security Categories, National Institute of Standards and Technology (NIST), 1 revision, vol. I, 53 pages. NIST Special Publication 800-60 (August 2008)
15. Jean DerGurahian, Data privacy and Security, SearchHealthIT.com (April 2011)
16. Robert Richardson, CSI Director, CSI Computer Crime and Security Survey (2010, 2011), http://www.GoCSI.com