International Journal of Advance Research in Science and Engineering
Volume No.07, Special Issue No.04, March 2018
www.ijarse.com
IJARSE
ISSN: 2319-8354

PRIVACY PROTECTION AND SECURITY CHALLENGES IN ELECTRONIC HEALTHCARE RECORDS

Musavir Hassan[1],Muheet Ahmad Butt[2], MajidZaman[3]

Research Scholar, University of Kashmir, Hazratbal Srinagar [1]

Post Graduate Department of Computer Science, University of Kashmir, Hazratbal Srinagar [2]

Post Graduate Department of Computer Science, University of Kashmir, Hazratbal Srinagar [3]

ABSTRACT

Electronic Health Records promise to solve many of the current healthcare challenges since they have the potential to improve performance and quality of healthcare. These EHRs can perfectly diagnose diseases if utilized appropriately. Although the EHRs can possibly resolve many of the existing problems connected with disease diagnosis, however, the main obstacles in effectively using them are the patient privacy, security and integrity of healthcare data.Due to these concerns even if dissemination of Electronic Health Records (EHRs) can be highly beneficial for a range of medical studies, spanning from clinical trials to epidemic control studies, but EHRs may be still prone to breaches that threaten patient privacy that has hampered some of the significant advantages of using EHRs. In this work, we present the state-of-art Electronic health record system. We review the algorithms, derive insights on their operation, and highlight their advantages and disadvantages. The review uncovers many opportunities and challenges for improving privacy and security measures in future and also determine that getting privacy and security right have a significant impact on the success of Electronic Health Records.

Keywords: Privacy, Security, Electronic Health Records, Integrity

1. Introduction

An electronic health record (EHR) is a digital record of apatient's medical details. It encompasses full range of data relevant to a patient's care such as demographics, problems, medications, physician's observations, vital signs, medical history, immunizations, laboratory data, radiology reports, personal statistics, progress notes, and billing data.Now a day's physicians and hospitals are implementing EHRs with high pace because they offer several advantages over paper records.They helps to improve the quality and convenience of patient care, increase access to health care, and improve the accuracy of diagnosis and health outcomes.Althoughthe dissemination of patient data is greatly beneficial, but it contains confidential and sensitive data so it must be performed in a way that preserves patient's privacy. [1]

2. The State of the Art of Security and Privacy in EHR

Over the years healthcare systems were single, isolated units however at presentEHR's are large, diverse, interoperable, integrated systems. With this development of technology, cloud has been spotted as a solution for healthcare practitioners to implement interconnected EHR extensively to ensure continuity of care. We present three significant technologies demonstrating the big splash in medical information technologies and the security and privacy challenges they pose.

Health sensing: There's been a sharp increase in the quantity and variety of consumer devices and medical sensors that capture some aspect of physiological, cognitive, and physical human health. The implementation of these technologies empowers the end users (e.g., chronic patients) by providing means to monitor and record the status continually and, if the need arises, seek remote assistance [2].

Big data analysis in healthcare: With the increasing digitization of health care, a large amount of healthcare data has been accumulated and the size is increasing at an unprecedented rate. Discovering the deep knowledge and values from the big healthcare data isthe key to deliver the best evidence-based, patient-centric, and accountable care [3].

Cloud computing in healthcare: With healthcare providers looking at solutions to lower the operating costs, emerging technologies such as cloud computing can provide an ideal platform to achieve highly efficient use of computing resources, simplify management, and improve services. Cloud computing can support the analysis of the big data. There is no doubt that the adoption of these innovative technologies in medical fields can create significant opportunities. Nevertheless, many challenges still need to be addressed in order to achieve truly enhanced healthcare services,especially security and privacy [4]. Accountability and auditing when medical records are accessed and manipulated must be provided by the EHR's. Therefore, there must be a system of checks and balances that is implemented and followed religiously but which continues to allow the data access necessary to perform a task.

3. Components of Electronic Health Record (EHR)

Mostly EHR's are designed for each service a patient receives from an auxiliary department, such as radiology, laboratory, or pharmacy, or as a result of administrative action. Some EHR's also allow electronic capture of physiological signals (e.g., electrocardiography), nursing notes, physician orders, etc. Often, these electronic records are not integrated; they remain as individual systems, which each have their own user log-ins and their own patient identification systems. Figure 1 illustrates a set of individual systems.

International Journal of Advance Research in Science and Engineering
Volume No.07, Special Issue No.04, March 2018
www.ijarse.com
IJARSE
ISSN: 2319-8354

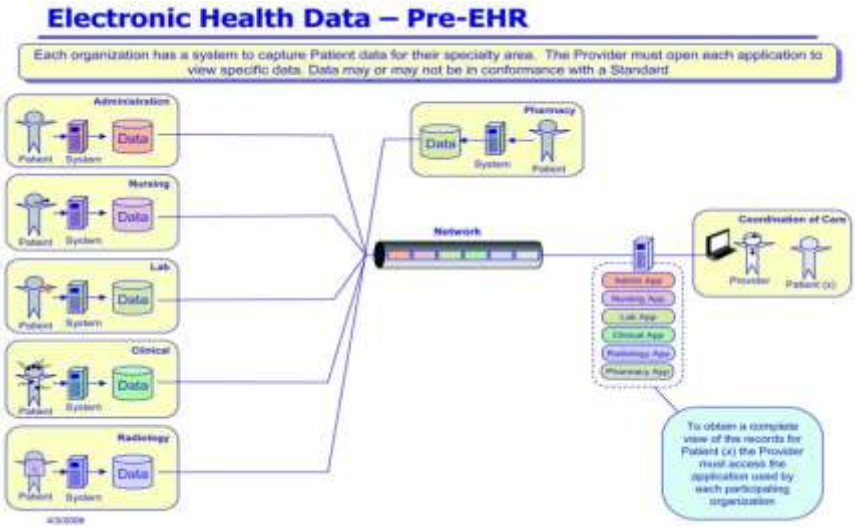

Fig1. Electronic Health Data- Pre EHR

To allow sharing of data across systems an integrated architecture can be created. Each system in Figure 2 stores its own data locally. To share patient information, a system (or system user) must allow another system to access its files, or it must transmit a copy of the file to the other system.Depending upon the level of interoperability between the integrating systems, files can be integrated with other files. The EHR in Figure 2 depicts the integration of healthcare data from a participating collection of systems for a single patient encounter.

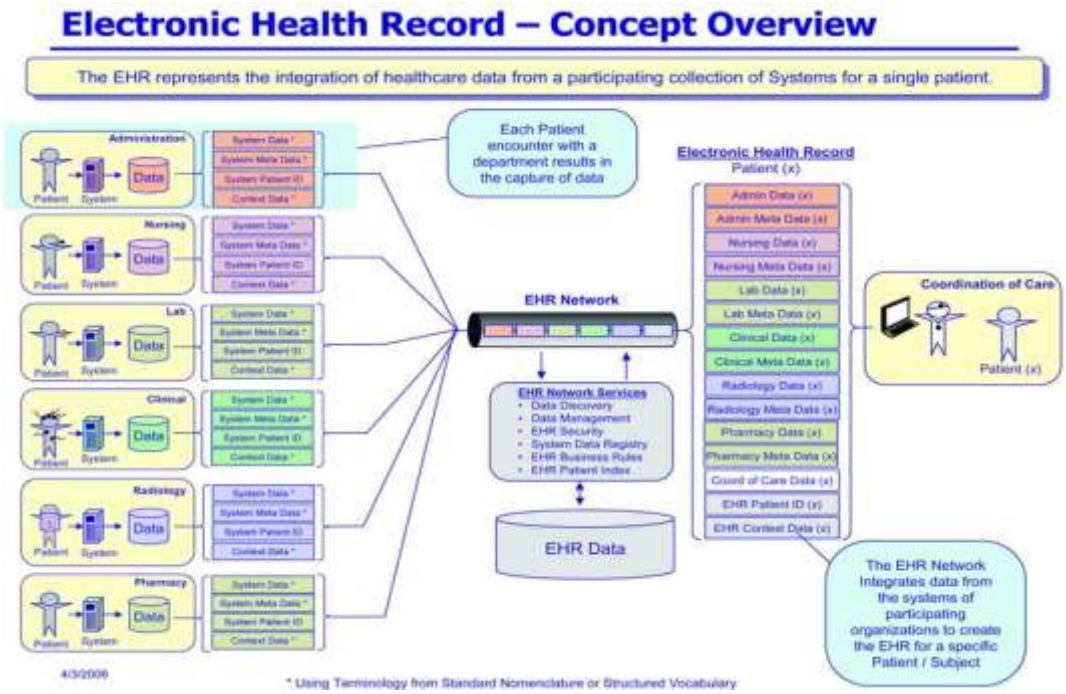

Fig. 2 EHR Concept overview

The number of integrated components and features involved in any given EHR is dependent upon the data structures and systems implemented by the technical teams. Following are the basic components of EHR.

3.1 Administrative System Components

The fundamental component of the EHR is administrative system component (patient registration, admission, discharge, and transfer data). This component includes vital information for accurate patient identification and assessment such as demographics, employer history, chief compliant,patient disposition, etc., along with the patient billing information. It may also include Social history data such as marital status, home environment, daily routine, dietary patterns, sleep patterns, exercise patterns, tobacco use, alcohol use, drug use and family history data such as personal health history, hereditary diseases, father, mother and sibling(s) health status, age, and cause of death. During the registration process, a patient is generally assigned a unique identification key comprising of a numeric or alphanumeric sequence.

3.2 Laboratory System Components

Generally laboratory systems are standalone systems that are used as hubs to integrate orders, results from laboratory instruments, schedules, billing, and other administrative information. Laboratory data is integrated entirely plays an extremely important part in the clinical care process, providing professionals the information needed for prevention, diagnosis, treatment, and health management. About 60% to 70% of medical decisions are based on laboratory test results [5]. A physician can easily compare the results from previous tests. If the options are provided, hecan also analyze automatically whether data results fall within normal range or not.

3.3 Radiology System Components

Radiology system components are used by radiology departments for managing medical imagery and to tie together patient radiology data (e.g., orders, interpretations, patient identification information). The typical Radiology system components will include patient tracking, scheduling, results reporting, and image tracking functions. RIS systems are usually used in conjunction with picture archiving communications system (PACS), which is a medical technology for providing economical storage and convenient access to the digital images. Although many hospitals are using RIS, it may or may not be integrated with the central EHR system.

3.4 Pharmacy System Components

In hospitals and clinics, Pharmacies are highly automated to maintain the inventory, prescription management, billing, and dispensing medications. It will also hold the complete medication history of a patient such as drug name, dosage, route, quantity, frequency, start and stop date, prescribed by, allergic reaction to medications, source of medication, etc. Again, it may be independent of central EHRs and also assure safe and effective medication and supporting patient-centered care.

3.5 Computerized Physician Order Entry

Computerized Physician Order Entry (CPOE) is a very important part of EHRs that permits a medical practitioner to enter medical orders and instructions for the treatment of a patient. CPOE systems offer a range of functionality, from pharmacy ordering capabilities alone to more sophisticated systems such as complete ancillary service ordering, alerting, customized order sets, and result reporting. As a digital system, CPOE has the potential to reduce medicationrelated errors. It is possible to add intelligent rules for checking allergies, contradictions, and otheralerts. The primary advantages of CPOE are the following: overcomes the issue of illegibility, fewererrors associated with ordering drugs with similar names, more easily integrated with decision supportsystems, able to link the adverse drug event (ADE) reporting systems, able to avoid medicationerrors like trailing zeros, create data that is available for analysis, point out treatment and drug ofchoice, reduce under- and overprescribing, and finally, the prescriptions can reach the pharmacyquicker. While ordering, a professional can view the medical history, current status report from adifferent module, and evidence-based clinical guidelines. Thus, CPOE can help in patient-centeredclinical decision support.If used properly, CPOE decreases delay in order completion, reduces errors related to handwritingor transcriptions, allows order entry at point-of-care or off-site, provides error checking forduplicate or incorrect doses or tests, and simplifies inventory and positing of charges. Studies haveshown that CPOE can contribute to shortened length of stay and reduction of cost [6].

3.6 Clinical Documentation

Electronic clinical documentation systems enhance the value of EHRs by providing electronic capture of clinical notes; patient assessments; and clinical reports, such as medication administration records (MAR). As with CPOE components, successful implementation of a clinical documentation system must coincide with a workflow redesign and buy-in from all the stakeholders in order realize clinical benefits, which may be substantial as much as 24 percent of a nurse's time can be saved.15A clinical document may include [7]

- Physician, nurse, and other clinician notes
- Relevant dates and times associated with the document
- The performers of the care described
- Flow sheets (vital signs, input and output, and problems lists)
- Perioperative notes
- Discharge summaries
- Transcription document management
- Medical records abstracts
- Advance directives or living wills
- Durable powers or attorney for healthcare decisions
- Consents (procedural)
- Medical record/chart tracking
- Release of information (including authorizations)

• Staff credentialing/staff qualification and appointments documentations

• Chart deficiency tracking

• Utilization management

• The intended recipient of the information and the time the document was written

• The sources of information contained within the document. The clinical document architecture (CDA) is an XML-based electronic standard developedby the Health Level 7 International (HL7) to define the structure. It can be both read by human eyesand processed by automatic software.

4. Advantages and Disadvantages of EHR

This section discusses solutions for privacy protection of EHR inhospitals in the era of Nanobased technologies.Only technical solutionsare not enough, as they require a relatively high level of knowledge and technicalexpertise on the part of the patient. By addressing policy and legislation issuesdirectly, rather than combating sophisticated protection techniques, we may producereasonable and acceptable solutions that outlast today's technology circle.There are a lot of advantages of using EHRin health care examined by the researchers such as significantreduction in healthcare costs, reduction in medical errors, and improved quality ofcare. In order for these advantages to be realized, an electronic health records must beconnected and integrated to provide anytime, anywhere healthcare information anddecision support via a comprehensive knowledge-base of interoperable systems.Other potential secondary benefits of EHR adoption is the reduction of care variabilityby using data to define and disseminate best practices, therefore helping todeliver more effective care to a broader patient base [8]. In addition, consumer andpatient interfaces with EHR systems may yield valuable data that might provideadditional benefits such as "determining provider (hospital and physician)performance outcomes, monitoring chronic diseases, monitoring medicationadherence, promoting safety metrics, determining patient satisfaction, promotingmore informed clinical decisions, and improving patient–physician communicationtracking" [9].These and other challenges lead to unintended consequences of advantages ofusing EHR, such as the ones pointed out in [10], which author terms harmfulshortcuts(i.e., copying and pasting of data obtained from other physicians, authorshipambiguities, inadequate discharge summaries, and impaired physicians–patientcommunication).The introduction and use of EHR can have a profound effect on medical malpracticeliability. For example, in [11] author explored this area and raisedseveralpoints regarding the new responsibilities medical staff and service providerswill have to bear following adoption of e-Healthcare Systems including the documentationof clinical findings, the recording of test results, and the use of clinical decision support systems. Should errors arise during the use of the system how willthe players be held accountable? The temptation to copy and paste past entries insteadof retaking medical histories still exists, and may result in a failure to incorporatenew information and the perpetuation of the past mistakes.The use of ICT and medical devices in EHR generates hugeamount of data that are easily available to healthcare professionals. There is a schoolof thought emerging, advancing the argument that this new and easier

access toinformation may also lead to an overload that could cause the healthcare professionalsto miss important items of information. This has impact on malpractice litigationprocesses, because the information now available to healthcare professionalsis also available to the legal authorities. Integrating clinical systems into practice mayredefine the standards of care and provide definite objective answers to previously ambiguous questions, which were caused by incomplete or fuzziness in data. [12] Show that it is possible to generate medical reports that areacceptable by health professionals automatically from breast medical images. Theyfurther argue that their proposed method should be useful in general doctors' practice,wherein there is a predefined set of medical descriptors to be acquired by a doctorduring image investigation. This means automatic information generated fromimages can enable doctors with little training in reading breast medical images toprovide initial informed opinion to patients.The World Health Organization predicts that chronic diseases will account foralmost three-quarters of all deaths worldwide by 2020 [13], so the evolution ofM-Health (mobile diagnostics, bio-feedback, and personal monitoring) is set to revolutionizetreatment of conditions such as diabetes and high blood pressure. Appsdesigned by medical professionals will provide efficient real-time feedback, tacklechronic conditions at a much earlier stage, and help to improve the lifestyles and lifeoutcomes of communities in the developed and developing world [14].[15] Proposesthe balanced p+-sensitive k-anonymity and balanced (p,α)-sensitive k-anonymity model, which are extensions of the$p$+-sensitive k-anonymity and (p, α)-sensitive k-anonymitymodels.However, the disadvantages are many such as significant losses of personalinformation privacy as a result of poorly configured systems, defective safeguards byhealthcare providers, or negligent technical system design without satisfactory securitysafeguards. Other disadvantages include medical identity theft, marketing firms,employer and insurance companies accessing medical data, and sharing of medicalinformation without patient knowledge and consent. Other obstacles limiting thedeployment of EHR systems are funding, technology, attitude, and organizationalaspects [16]. Overall, more research is needed to determine the best way to implementthe system so that it will interfere as little as possible with doctor's daily flow.

5. Privacy and security challenges in EHR

Privacy and security challengeshave existed over years mostly in financial institutions. However the focus has now shifted towards healthcare industry due to enormous amount of sensitive information.

5.1 Privacy challenges in electronic health records:

EHR holds patients health data which is regarded as very sensitive and therefore such systems holding this information should be in position to follow the golden rule of confidentiality, Integrity and Availability to lower chances of data compromise, inform of theft, data breaches and physical attacks and hacking among others [17].

Data Breaches

According to a survey conducted in UK, it is identified that over 75% of patients are inquisitive on how their health data is shared with third party organization and/or stored. The perception in patients may be due to the fact that health data has been reported as the most targeted data by hackers and cyber criminals [18].Healthcare industry and

companies processing health related information still remain the most targeted sector as it holds highly valued data which is also exposed to vulnerabilities through mobile and IOT devices. Moreover, 89% of the data breach identified are fueled by a financial motive[18]says medical records are 10 times worth compared to credit cards numbers. Security breaches might be subjected to a jail term as per the HIPPA rules and regulations if the responsible party is identified. Furthermore the data breach report from the office of civil Rights emphasized that healthcare sector was one of the highly affected domain. The report further stated that, a total of 155 million records of patients were exposed to public as a result of in appropriate measure to implement security controls on the system holding the data.

EHR considered dealingwith two identified aspects of privacy; contextual oriented privacy and content oriented privacy. The ability of malicious parties to identify what kind of sickness a patient has is referred as contextual oriented privacy. This is normally achieved through investigating the field of the patient's physician.On the otherhand content oriented privacy specifies the likelihood of stakeholders in healthcare organization's to disclose patients sensitive data to other parties for instances, insurance companies and marketing agencies without patient consent

Patient Data visibility

As identified in the existing HIPPA privacy rule, patients should have full visibility of how their health records are used and for what purposes. However this aspect has not been fully addressed by concerned parties and continues to be under violation. This is because, it is impossible for patients to oversee the usage of their health data unless they are included in the access control. In [19] author argues that patient's involvement in management of their own health data in EHR would probably improve the privacy issues

5.2 Security Challenges in electronic health record:

Security of healthcare information commences with the protection of patient medical records by guaranteeing that privacy, confidentiality and integrity of the EHR system is maintained at all times[19] Technology advancement is rapid as never before, however the aspect of privacy concern in EHR still remains unclear towards consumers as a result of prevailing breach thus lowering the trust of the systems[20]. In this research, three categories of security challenges have been identified and included: human factors, law and ethics, and CIA protection.

Human Factors:

According to a study conducted by KTH University research students in Sweden over physicians, it was identified that around 76% of them considered human factor as the ultimate challenge in EHR implementation whereas 53% had little or no interest in health IT. Therefore, EHR systems have a higher probability of being successfully implemented if the usability study is carried out beforehand adopting to the healthcare environment.

Robert further identifies human element as an important aspect in information security and privacy. The people interaction to medical data in the system should be considered during the design of EHR [21]. Since the current security threats are mostly associated with human aspects to the system. Thus sufficient training to staff on the EHR usage and the need for patient's privacy requirements has to be addressed.

Law and Ethics

According to the exploratory study in the USA regarding third party access to medical records, it is argued that government should be able to override the disclosure of patient's privacy policies to third party organizations. In the case of the disease outbreak, the govt. is supposed to coordinate with the research agencies to make sure that the consumption of medical data are dealt with the best possible way without affecting the privacy of patients thus improving the quality of healthcare delivery.

Although, a number of rules and regulations both at the state and federal level have been established to protect patient privacy for instance. HIPPA Health information Technology for Economics and clinical health (HITECH) to leverage implementation of health IT infrastructure, privacy preservation of data is still questionable[22].

Confidentiality, Integrity and Availability Protection

As healthcare organization transforms paper charts into computerized records through the use of EHR system, security breaches will always be a concern as this compromises the integrity and confidentiality of the health records[23]. As a result generic requirements for EHR systems have been provided by the international directives such as HIPAA, European Data Protection and requires EHR implementation to satisfy the CIA trade. Below is the definition of CIA in HER security requirements [24].

Confidentiality

This refers to the ability to safeguard information in the EHR system so that it can only be accessed by authorized subjects. Typically authorized subjects will gain access based on the predefined role based privileges. Therefore no information should be released without their consent unless otherwise as stated by privacy rule. Authorization is mainly carried out by a security mechanism called an "access control".

Integrity

Integrity can be understood by preserving the initial representation of data even in the case of any alterations [25]. Ensuring integrity is key in EHR system since it guarantees the accuracy of data thus minimizing errors and improving the safety of patients [19]. Currently authorized users can also participate in creating in accuracies if inadequately trained on the use of the for instance, the use of cut and paste feature. Drop down menus have also been reported as one of the main cause of data inaccuracies in HER.

Availability

The system should be able to be accessed any time when required by authorized parties and entities for example in the case of any emergency situation and specific physicians need access to patient's record to carry out diagnosis and approve medication to a patient. The systems should not be constrained to a specific time of the day otherwise the physician's job will be made complex since decisions can't be made in real time as required[22].

6. Conclusion

In our increasingly data-driven society, privacy and security are the most challenging issues. Although EHRs are increasingly used by patients, doctors and other healthcare professionals because of several advantages, but it bring several privacy, security and integrity problems together. In this article,our key contribution is to present state-of-the-art approaches regarding security,privacy, and integrity aspects of EHS by considering the components andchallenges of e-health services.The review uncovers many opportunities and challenges for improving privacy and security measures in future and also determine that getting privacy and security right have a significant impact on the success of Electronic Health Records.

REFERENCES

[1] AkhilShenoy, Jacob M. Appel. Safeguarding Confidentiality in Electronic Health Records. Bioethics and Information TechnologyCambridge Quarterly of Healthcare Ethics.2017;26: 337–341.

[2] Zheng Y.L., Ding X.R., Yan Poon C.C., Lai Lo B.P., Zhang H., Zhou X.L., et al. Unobtrusive sensing and wearable devices for health informatics. IEEE Transactions on Biomedical Engineering. 2014; 61(5): 1538–1554.

[3] Murdoch T.B., Detsky A.S. The inevitable application of big data to health care. Journal of the American Medical Association. 2013; 309(13): 1351–1352.

[4] AbuKhousa E., Mohamed N., Al-Jaroodi J. e-Health cloud: Opportunities and challenges. Future Internet. 2012; 4: 621–645.

[5] HL7: Medical Records/Information Management. http://www.hl7.org/.

[6] Hagop S. Mekhjian, Rajee R. Kumar, Lynn Kuehn, Thomas D. Bentley, Phyllis Teater, Andrew Thomas, Beth Payne, and Asif Ahmad. Immediate benefits realized following implementation of physician order entry at an academic medical center. Journal of the American Medical Informatics Association.2002; 9(5):529–539.

[7] Electronic health records overview. National Institutes of Health National Center for Research Resources, MITRE Center for Enterprise Modernization, McLean, Virginia, 2006.

[8] Jha A.K., Adler-Milstein J. Regional Health Information Organizations and Health Information Exchange. In: Blumenthal D., ed. Health Information Technology in the United States: Where We Stand. BMJ Publishing Group Limited, Harvard University, Cambridge, MA, 2008; p. 8.

[9] Donelan K., Miralles P.D. Consumers, EHRS and PHRs: Measures and Measurement. In: Blumenthal D., ed. Health Information Technology in the United States: Where We Stand, Robert Wood Johnson Foundation, Princeton, NJ, 2008; pp. 56–57.

[10] Bernat J.L. Ethical and quality pitfalls in electronic health records. Neurology. 2013; 80 (11): 1057–1061.

[11] Mangalmurti S.S., Murtagh L., Mello M.M. Medical malpractice liability in the age of electronic health records. New England Journal of Medicine. 2010; 363(21): 2060–2067.

[12] Kisilev P., Walach E., Barkan E., Ophir B., Alpert S., Hashoul S.Y. From medical imageto automatic medical report generation. IBM Journal of Research and Development. 2015; 59(2/3): 2:1–2:7.

[13] WHO. The global burden of chronic. 2015. Available at: http://www.who.int/nutrition/topics/2_background/en/ (accessed on May 9, 2015).

[14] AdeelAnjum , SaifurRehman Malik , Kim-Kwang Raymond Choo, Abid Khan , AsmaHaroonet al. An efficient privacy mechanism for electronic health recordscomputers & s e c u r i t y. 2 0 1 8; 196–211.

[15] Howard J. 7 Top futurists make some pretty surprising predictions about what the next decade will bring. 2015. Available at: http://www.huffingtonpost.com/2015/05/12/ futurists-next-10-years_n_7241210.html (accessed on May 9, 2015).

[16] Fernandez-Alemán J.L., Señor I.C., Lozoya P.Á.O., Toval A. Security and privacy inelectronic health records: A systematic literature review. Journal of Biomedical Informatics. 2013; 46(3): 541–562.

[17] Maslin,M and R.Ailar, Cloud computing adoption in Healthcare sector: A SWOT analysis can center Sci. Educ.2015 ; 11: 12-18

[18] Papoutsi, C., J.E. Reed, C. Marston, R. Lewis and A Majeed et al. Patient and public views about the security and privacy of Electronic Health Records (EHRs) in the UK: Results from a mixed method study.BMC. Med Inf. Decis. Making. 2015; 15: 1-15

[19] Appari, A. and M.E Johnson, Information security and privacy in healthcare: Current Sate of research Int. J. InternetEnterp. Manage.,2010.; 6: 279-314

[20] Jacob, J. V. Agrawal,. Privacy in Electronic Health Record systems consumer's perspective Stockholm University, Stockholm, Sweden.2010.

[21] Dlamini, M.T.,J.HEloff and M.M Eloff,. Information Security. The moving target. Computer Sec., 2009;28: 189 – 198

[22] Sicuranzsa, M., A Esposito and M. Ciampi,. A semantic access control for easy management of the privacy for EHR systems. Proceedings of the 9th International Conference on P2P Parallel Grid Cloud and internet computing(3PGCIC) 2014; November 8-10, 2014, IEEE, Naples, Italy, ISBN: 978-1-4799-7872-4, pp.: 400-405

[23] Bennani, A., M.Belalia and R.Ournlil. As a human factor, the attitude of healthcare practioners is the primary step for the E health: First outcome of an outgoing study in Morocoo. Column, IBIMA., 2008; 3: 28-34

[24] Ferreira, A., C.R. Cruz and L. Antunes. Usability of authentication and access control: A case study in healthcare. Proceedings of the 2011 IEEE International Conference on carnahan security Technology (ICCST), October 18-21, 2011, IEEE, Porto, Portugal, ISBN:978-1-4577-0902-9,pp:1-7.

[25] Fernandez-Aleman, J.L.,I.C. Senor, P.A.O. Lozoya and A. Toval, Security and Privacy in electronic health records: A systematic literature review. J. Biomed. Inf, 2013;46: 541-562