JOURNAL OF CRITICAL REVIEWS

ISSN- 2394-5125 VOL 6, ISSUE 04 , 2019

# ADVANCEMENTS TO HOSPITAL CYBERSECURITY WITH HEALTH INSURANCE: CRITICAL ANALYSIS

**Janne Umapathi[1], Dr. Vishal Khatri[2]**

[1]Research Scholar, Department of Computing and Information Technology, Himalayan University, Itanagar, Arunachal Pradesh, INDIA.

[2]Research Guide, Department of Computing and Information Technology, Himalayan University, Itanagar, Arunachal Pradesh, INDIA.

## Abstract

Keeping sensitive patient data safe is essential for hospitals and other medical facilities. Electronic Health Records (EHRs) are considered highly confidential documents at healthcare facilities due to the sensitive nature of the information contained inside them. The proper handling of sensitive patient data is essential to preventing its disclosure or misuse. The purpose of this research is to analyze the current state of information security management practices with regard to Electronic Health Records (EHR) and how they are safeguarded against potential security threats and risks in healthcare, especially when communicating sensitive information between various healthcare actors and across borders. In order to identify potential difficulties connected to security threats to healthcare management, a case study and various interviews were conducted on the Indian healthcare system. The theoretical work laid the groundwork and offered justification for possible remedies to security concerns and threats in Indian healthcare. Following the completion of the mapping process, potential rules and recommendations were created for healthcare institutions to follow in order to prevent unwanted access to sensitive information and maintain information security. Data security threats in the Indian healthcare system were analyzed, and recommendations were made to improve the state of affairs and head off future threats. We can now say that the technical and administrative handling of security issues has been thoroughly investigated. Its primary function is healthcare, and it is the obligation of the company's upper management to protect the privacy of patients' personal data.

***KEYWORDS:*** *Information Security, Electronic Health Records, Intellectual Communications Technology*

## Introduction

Patient information stored in Electronic Health Records (EHRs) or patient electronic journals is the most significant information for healthcare institutions to have. The residents of this country value access to high-quality medical treatment. Accordingly, healthcare administration needs a dependable format for handling EHR and patient data. There is a high degree of delicateness in the current patient data and information. It is the goal of a healthcare management system with a well-structured database of sensitive data to facilitate the distribution of timely and relevant information to the right people and places to provide the best possible conditions for providing care [1-5].


**Figure 1:** Information security management ensures that the appropriate information is delivered to the appropriate location and person at the appropriate time.

Figure 1 shows how an information security management system can help guarantee that patients get the best possible medical care. As an added bonus, a healthcare system built on the latest technological advancements also increases the accessibility, usability, and availability of relevant data and tools. Many different strategies for managing data in accordance with stakeholder needs are implemented within the electronic management system [5-11]. Users of an electronic information system should have access to their data or Electronic Health Records (EHRs) regardless of the institution they are affiliated with. Patients have received more high-quality care since the introduction of EHR systems in the medical field and during Covid times [12-17]. Therefore, possible security threats to sensitive information in healthcare could endanger both patient privacy and safety.

## Research Methodology

To begin, we employ a descriptive research technique that will allow us to collect and handle data. After the data was collected, we would look into it and analyze what we found. You can either conduct primary research or rely on already-existing information to fill in the gaps. Secondary data was compiled from a variety of studies, policy briefs, and the media for this research.

## Research approach

Case studies show that face-to-face meetings are crucial for sharing knowledge throughout businesses. To determine the information security threats connected with electronic health records, the authors conducted many interviews with staff members of the Indian County healthcare system (EHR).

Through conducting in-depth interviews with key players in the health care system, we were able to collect qualitative data on a wide range of activities and look for areas where ICT may be improved (ICT). Among these were members of upper management and administration, as well as doctors and technical administration (IT staff). The author gathered data on the healthcare provider's approach to information security by asking a series of carefully crafted questions. During the interview, several questions and conversations were used to elicit data regarding the targeted field. We made notes and recorded the interviews so that we could analyze the data afterwards.

ISSN- 2394-5125 VOL 6, ISSUE 04 , 2019

## Population and sample

### Sampling

There should be at least one primary care clinic, one secondary care clinic, and five intermediate and tertiary care clinics in each level. The best-case scenario is if they were selected at random. Generally speaking, it might make the most sense to Centre efforts on infrastructure that improves participation in research activities (survey). Study units are the hospitals and clinics that were used to collect data.

### Target audience definition (health sector personnel)

The number of workers at each study unit (health facility or source of service providing ambulatory or home care) should be listed. Facilities may maintain a provisional list of personnel employed at that location. The researcher should make every effort to obtain an accurate and complete list of the target population.

### Population stratification (grouping personnel)

It is important to properly categorize the people listed in the chosen study units. Differentiating between nurses, receptionists, doctors, security guards, etc. The research protocol's personnel types are described in greater detail on page 3. Depending on the specifics of the situation, these classifications may need to be revised.

### The sample sizes

Due to the breadth of variables being studied, statisticians advise collecting data from at least 1,000 people in each country. Some nations may struggle to do this in the allotted time frame and with the given resources. Researchers are tasked with proposing an appropriate sample size and providing an explanation for why a smaller sample size was selected.

### Research tools

Features that are helpful to public health professionals can be found in other NLM resources. MEDLINE is an especially helpful resource. Medical, nursing, dental, public, and veterinary health; the health care system; preclinical sciences; and much more are all covered in this comprehensive bibliographic database from the National Library of Medicine.

### Data collection method

After patients were released from the hospital, two research assistants looked through their scanned medical records to see what information was still relevant. Any interested parties may then access this file through computer. The major source of information is the patient's medico-legal record upon admission, which has been utilized as a gold standard measure for other outcomes like diagnostic accuracy and adverse event rates but not for hospital length of stay or discharge destination.

### Statistical analysis

Quantitative and qualitative information gathered through various channels was described using descriptive statistics.

ISSN- 2394-5125 VOL 6, ISSUE 04 , 2019

## Results

Security models, methodologies, and applications have proliferated in the recent decade in response to the growing prevalence of information and communication technologies (ICTs), with the ultimate goal of reducing vulnerability and thwarting attack. Although many new electronic health care applications have been made possible by the rapid growth of IT, whether or not they can ensure the privacy of patients' medical records is an unanswered subject.

Therefore, we polled five individuals working in the healthcare industry in India over three separate interviews. The head nurse in the psychiatry department, with the help of a qualified coordinator, conducted the initial interview. The second discussion involved the chief of IT policy maker management at India County Health Care and his law and policy advisor. Finally, an IT engineer conducted the interview; the candidate was looking for a position in IT related to data protection.

1 Procedure for Access Control (availability and accessibility)
2 India Healthcare's Electronic Health Records (EHR)
3 Health care legislation, standards, and guidelines
4 Communication of sensitive information across borders
5 Information Security Awareness in India.
6 Patient Privacy and Safety in Healthcare in India.

## Risk Assessment and Management

Electronic journals and electronic health records contain personal information about patients; therefore, healthcare providers must be able to handle and protect that data with care. This is a safety precaution taken to protect the administration of the system from harm.

## India Healthcare's policies and procedures, as well as applicable laws and standards

In accordance with Swedish constitutional law, the senior management in India Country is solely responsible for enforcing the organization's health care information security policies and procedures. Health data security is compromised due to a lack of available, adequate, and comprehensive standards, policies, and procedures. The Swedish Constitution, the National Board of Welfare, and the Ministry of Health and Social Affairs govern all health care organizations in India.

## Conclusion

The article concludes by stressing the significance of healthcare information security in terms of patient safety (patient safety and patient secrecy). India's healthcare system, specifically its electronic patient journals and Electronic Health Record (EHR), is the primary focus of this research. This is so that proper security measures can be taken to allow authorized users only to access the relevant data and prevent any outsiders from gaining access.

## References

1) Aburayya, A., Alshurideh, M., Al Marzouqi, A., Al Diabat, O., Alfarsi, A., Suson, R., Bash, M. and Salloum, S.A., 2020. An empirical examination of the effect of TQM practices on hospital service quality: an assessment study in UAE hospitals. *Syst. Rev. Pharm, 11*(9), pp.347-362.
2) Habibzadeh, H., Nussbaum, B.H., Anjomshoa, F., Kantarci, B. and Soyata, T., 2019. A survey on cybersecurity, data privacy, and policy issues in cyber-physical system deployments in smart cities. *Sustainable Cities and Society*, *50*, p.101660.

3) Barasa, E., Rogo, K., Mwaura, N. and Chuma, J., 2018. Kenya National Hospital Insurance Fund Reforms: implications and lessons for universal health coverage. *Health Systems & Reform*, *4*(4), pp.346-361.
4) Abraham, C., Chatterjee, D. and Sims, R.R., 2019. Muddling through cybersecurity: Insights from the US healthcare industry. *Business horizons*, *62*(4), pp.539-548.
5) Burkle Jr, F.M., 2019. Challenges of global public health emergencies: development of a health-crisis management framework. *The Tohoku journal of experimental medicine*, *249*(1), pp.33-41.
6) Maphumulo, W.T. and Bhengu, B.R., 2019. Challenges of quality improvement in the healthcare of South Africa post-apartheid: A critical review. *Curationis*, *42*(1), pp.1-9.
7) Pandey, S., Singh, R.K., Gunasekaran, A. and Kaushik, A., 2020. Cyber security risks in globalized supply chains: conceptual framework. *Journal of Global Operations and Strategic Sourcing*.
8) Akter, S., Michael, K., Uddin, M.R., McCarthy, G. and Rahman, M., 2020. Transforming business using digital innovations: The application of AI, blockchain, cloud and data analytics. *Annals of Operations Research*, pp.1-33.
9) Porcedda, M.G., 2018. Patching the patchwork: appraising the EU regulatory framework on cyber security breaches. *Computer law & security review*, *34*(5), pp.1077-1098.
10) Bhuyan, S.S., Kabir, U.Y., Escareno, J.M., Ector, K., Palakodeti, S., Wyant, D., Kumar, S., Levy, M., Kedia, S., Dasgupta, D. and Dobalian, A., 2020. Transforming healthcare cybersecurity from reactive to proactive: current status and future recommendations. *Journal of medical systems*, *44*(5), pp.1-9.
11) World Health Organization, 2018. Continuity and coordination of care: a practice brief to support implementation of the WHO Framework on integrated people-centred health services.
12) Dasaklis, T.K., Casino, F. and Patsakis, C., 2018, July. Blockchain meets smart health: Towards next generation healthcare services. In *2018 9th International conference on information, intelligence, systems and applications (IISA)* (pp. 1-8). IEEE.
13) Khezr, S., Moniruzzaman, M., Yassine, A. and Benlamri, R., 2019. Blockchain technology in healthcare: A comprehensive review and directions for future research. *Applied sciences*, *9*(9), p.1736.
14) Abugabah, A., Nizamuddin, N. and Abuqabbeh, A., 2020. A review of challenges and barriers implementing RFID technology in the Healthcare sector. *Procedia Computer Science*, *170*, pp.1003-1010.
15) Napi, N.M., Zaidan, A.A., Zaidan, B.B., Albahri, O.S., Alsalem, M.A. and Albahri, A.S., 2019. Medical emergency triage and patient prioritisation in a telemedicine environment: a systematic review. *Health and Technology*, *9*(5), pp.679-700.
16) Dr. J. Rukumani. 2021. Analytical Study on role of nursing officers in curing covid pandemic https://www.tojqi.net/index.php/journal/issue/view/47 .
17) Dr. Loxmi Jamoh, Dr. Shagufa Amber. 2021. Transmitting Scientific and Regulatory Gap of Nanomedicines and Discusses Current Trends of Nanomedicines. https://www.dcth.org/index.php/journal/issue/view/8.