International Journal of Management, IT & Engineering
Vol. 9 Issue 3, March 2019,
ISSN: 2249-0558 Impact Factor: 7.119
Journal Homepage: http://www.ijmra.us, Email: editorijmie@gmail.com
Double-Blind Peer Reviewed Refereed Open Access International Journal - Included in the International Serial Directories Indexed & Listed at: Ulrich's Periodicals Directory ©, U.S.A., Open J-Gate as well as in Cabell's Directories of Publishing Opportunities, U.S.A

IMPLEMENTATION OF ENHANCED CYBER SECURITY ARCHITECTURE IN HOSPITALS TO IMPROVE THE HEALTH ASSURANCE SERVICES AND ITS IMPACTS: A CRITICAL STUDY

Adonis Thokalath Sunny[1], Dr. Vishal Khatri[2]
Department of Computer Science
[1,2]Himalayan University, Itanagar, Arunachal Pradesh

Abstract

Background:In healthcare organizations, information security plays a critical role. In healthcare organizations, the Electronic Health Record (EHR) containing patient information is regarded as extremely sensitive. Sensitive patient information must be managed in such a way that it is safe and secure from unauthorized access.Objective:Theobjective of this study is to examine current information security management practices in relation to Electronic Health Records (EHR) and how these are protected from potential security threats and risks in healthcare, particularly when sensitive information must be communicated between different healthcare actors and across borders.Materials and Methods:The Indianhealth care system was investigated using a case study and several interviews to ascertain potential issues relating to security threats to healthcare management. The theoretical work provided the framework and justification for potential solutions to security risks and threats identified in Indian healthcare. At the conclusion of the mapping process, possible guidelines and recommendations for healthcare were made in order to prevent unauthorized access to sensitive information and to maintain information security were made. Results:Indian healthcare was investigated for potential issues and some possible guidelines and suggestions in order to enhance current information security while avoiding unavoidable risks to sensitive healthcare information. Conclusion:Security issues were investigated in the management of technical and administrative bodies. It is primarily responsible for healthcare, and in general, the entire business is under this management's responsibility to manage sensitive patient information.

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

International Journal of Management, IT & Engineering
Vol. 9 Issue 3, March 2019,
ISSN: 2249-0558 Impact Factor: 7.119
Journal Homepage: http://www.ijmra.us, Email: editorijmie@gmail.com
Double-Blind Peer Reviewed Refereed Open Access International Journal - Included in the International Serial Directories Indexed & Listed at: Ulrich's Periodicals Directory ©, U.S.A., Open J-Gate as well as in Cabell's Directories of Publishing Opportunities, U.S.A

1.0 Introduction

The most critical information for healthcare organizations is patient information in the form of Electronic Health Records (EHRs) or patient electronic journals. The county's residents strive to receive high-quality care from healthcare providers. Thus, healthcare management must have a well-organized structure or form in place to manage patient data and Electronic Health Records (EHR) data in the system. Existing patient information and data can be classified as sensitive to manage. A well-organized structure of sensitive information in a healthcare management system aims to provide optimal care opportunities based on the delivery of the appropriate information to the appropriate location at the appropriate time [1-5].

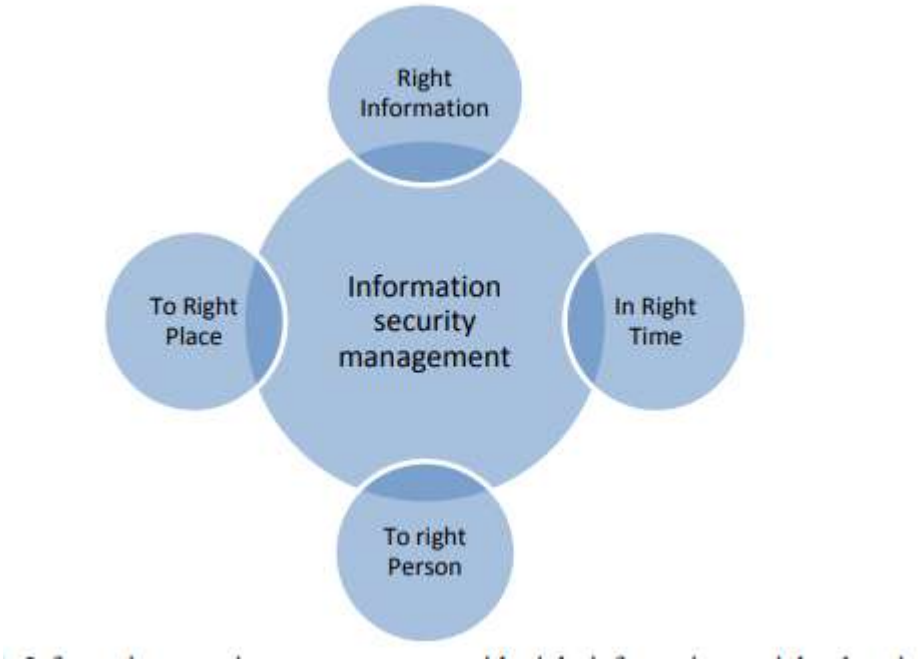

Figure 1: Information security management ensures that the appropriate information is delivered to the appropriate location and person at the appropriate time.

As illustrated in Figure 1, an information security management system should contain all necessary information and resources to ensure that patients receive high-quality health care. It is

possible if high-level information security is ensured in order for the system to deliver the correct information to the correct person at the correct time and in the correct location. When a healthcare organization lacks sufficient information about a patient's treatment or when that information is unavailable to management, it can result in patients receiving ineffective care. Because sensitive patient information is managed in a computerized environment in healthcare, high-level security requirements and requirements are required. Additionally, an electronic-based healthcare system improves information and resource availability, accessibility, and usability. The electronic-based management system makes several attempts to manage information in accordance with stakeholder requirements [5-11]. Through an electronic-based information system, users should be able to access their information or Electronic Health Records (EHRs) across organizational boundaries. The adoption of Electronic Health Records (EHR) in health care has resulted in an increase in the provision of high-quality care to patients. The evolution of computer-based systems Management of information security [12-22]. The Appropriate Information at the Appropriate Time to the Appropriate Person at the Appropriate Place 10 and implementation have benefited healthcare management, but they also pose a potential security risk and management risk. As a result, potential security threats to sensitive information in healthcare could jeopardize both patient privacy and security.

2.0 Research Methodology

We start with the strategy of descriptive research which allows us to data collecting and management. Following the collection of data, we would investigate and conduct an analysis of the whole sampling. These can be done in two ways; one is primary data collection whereas another is secondary data collection. The paper used secondary data gathered from various reports, policy briefs and news media.

2.1 Research approach

Face-to-face meetings are critical for gathering information within organizations, according to case studies. The authors conducted several interviews with employees of Indian County's health

care system to ascertain the information security risks associated with electronic health records (EHR).

Different actors in the health care system were interviewed in order to collect qualitative data about various activities and to attempt to identify potential deficiencies or shortcomings in health care's use of information communication technology (ICT). Three distinct interviews were conducted with various health care stakeholders in Indian County. These included senior management and administration, as well as physicians and technical administration (IT staff). The author used pre-planned questions to elicit information about the healthcare provider's information security management. Several questions were posed during the interview to elicit information about the specified domain, including informal discussion or questions. The interviews were taped to facilitate the ensuring analysis, and we took notes throughout.

Interviewing from the top down

In the county of IndiaWe used a top-down approach to conduct the interviews with various stakeholders in health care. Numerous levels must be dealt with in health care organizations for various business and dealings.

The top-level interview, which included top management and administration of healthcare providers, was conducted first to elicit information about management and how this area's strategy benefits the entire information communication system. Following consultation with senior management, the authors contacted a physician to conduct an interview regarding the availability, security, access control, and reliability of electronic health records, as well as the overall resources available to ensure safe and harmless treatment. Finally, management was interviewed who was in charge of the IT staff. At this level of contact, a thorough investigation and interview were conducted to ascertain how the management of ICT or IT staff views the provision of information security.

2.2 Population and sample

Sampling

Each category (strata) should have a minimum number of health facilities, at least one at the primary and secondary levels of care and five at the intermediate and advanced levels of care. The ideal situation would be for them to be chosen at random. In practice, it may be necessary to concentrate on facilities that facilitate access to research activities (survey). The sampled health facilities are referred to as study units.

Stage three: Using a stratified random sampling method, sample health sector personnel (target population) within selected study units.

(1) Identification of the target population (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.

(2) Population stratification (grouping personnel)

Personnel listed in the selected study units should be classified according to their professional groups. For instance, nurses/receptionists/physicians/guards/etc. should be classified separately. On page 3 of the research protocol, the personnel categories are listed. It is possible that these categories will need to be adapted to the local context.

(3) Stratified target population sampling

Following that, a separate simple random sample (SRS) can be drawn from each group.

The sample size

Experts in statistics recommend that each country have 1000 participants to ensure a statistically significant number of responses given the range of variables under investigation. This may be difficult for certain countries to accomplish within the time frame and resources available. Researchers are asked to propose a sample size that is realistic and to justify why they chose a smaller sample size.

2.3 Research tools

Additional NLM resources include features that are beneficial to public health practitioners. A particularly useful tool is MEDLINE (Medical Literature, Analysis, and Retrieval System Online). It is the National Library of Medicine's premier bibliographic database, encompassing the fields of medicine, nursing, dentistry, public health, and veterinary medicine, as well as the health care system and preclinical sciences.

2.4 Data collection method

Two research assistants conducted a retrospective review of scanned inpatient medical records following patient discharge. Within 48 hours of patient discharge, health record administrative staff scans all paper-based inpatient medical records to create an integrated digital record. This record is then available for electronic review. For the purposes of this study, the gold standard data collection method was a retrospective review of scanned inpatient medical records. This justification is based on the fact that the medico-legal record of the patient admission serves as the primary source of information and has previously been used as a gold standard measure for a variety of other outcomes such as diagnostic accuracy and adverse event rates, but not for hospital length of stay or discharge destination.

Pilot analysis

MEDLINE/PubMed provides filters that assist users in narrowing their search strategies to specific types of evidence or aspects of topics. The filters are largely based on N. L. Wilczynski et AL work. .'s Two new public health-related filters have been developed recently. Users can search for appropriateness, process assessment, outcome assessment, or clinical practice guidelines using the HSR Quality-Related Queries Using Research Methodology filter; users can also search for costs or economics using the HSR Cost-Related Queries Using Research Methodology filter.

2.5 Statistical analysis

Descriptive statistics were used to present the number and percentage of data collected via each data collection method.

Stata was used to conduct the statistical analyses (Version 13, StataCorp, and College Station, Texas, USA).

3.0 Results

Since the last decade's widespread adoption of ICTs, various models, techniques, and applications of security have been developed for evaluating resources and establishing security specifications with the goal of mitigating risk and avoiding system incidents. National Security Telecommunications and Information System Security (NSTISS) defines information system security as "the protection of information systems against unauthorized access to or modification of data, whether in storage, processing, or transit, as well as against denial of service attacks against authorized users or provision of service to unauthorized users, including those measures necessary to detect, document, and counter such threats." While the rapid advancement of information technology has resulted in the development of numerous electronic health care applications, it remains an open question whether the current system is capable of guaranteeing the security of sensitive healthcare information.

As a result, the findings from the interviews with the case study participants and the outcomes from various health care personnel were classified into distinct sections. These various categories include access control procedures (approach to ensuring that resources are available and accessible to legitimate users), healthcare Electronic Health Records (EHR), international and national standards, guidelines in accordance with India health care laws, cross-border information communication, patient privacy and secrecy, and awareness of information security knowledge.

As a result, we conducted three interviews with five different personnel from India health care. The initial interview was conducted by the head of the psychiatry department nurse with the assistance of a coordinated trained individual. The second interview was conducted between the head of IT policy maker management and his law and policy advisor at India county health care. Finally, the interview was conducted by an IT engineer, with the objective of obtaining an IT role concerned with information security.

1Procedure 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.

The following questions have been created by us.

RQ1: What are the information management issues in the investigated area in terms of information security?

RQ2: How could these issues be resolved to enhance healthcare information security?

3.1 Discussion

This section recommends us for explaining the theoretical work's findings using case studies (interviews) from our research. Essentially, the authors' agenda and discussion focused on information security in healthcare organizations. In our discussion, we must address several points that are critical to understanding the issue or problem of information security in India health care.

3.1 Risk Assessment and Management

Health care involves the handling of sensitive patient information, such as electronic journals and electronic health records, and quality security management and control quality expect much manipulation of all types of potential security risks to information security in healthcare providers. It is a precautionary measure designed to safeguard the system's management against potential threats.

3.1.1 Expected Access Control Issues (Authentication & Authorization)

3.1.2 Data Base's Expected Problem

3.1.3 Communication across Borders Expected Issues

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

In India County, only the organization's top management is responsible for enforcing health care information security policies and procedures in accordance with Swedish constitutional

legislation. Management's policies and procedures are intended to guide users' decisions and to educate personnel about their security responsibilities. Unavailable, insufficient, and limited standards, policies, and procedures create security risks for sensitive information in health care. In India, all health care organizations are regulated by the Swedish Constitution, the National Board of Welfare, and the Ministry of Health and Social Affairs

3.3 Ignorance

Security threats to health care assets can be generated as a result of insufficient knowledge and awareness of information security fundamentals, resulting in a variety of potential vulnerabilities in an organization's security.

4.0 Conclusion

This article concluded our contribution by emphasizing the importance of healthcare information security in terms of patient security (patient safety and patient secrecy). The primary area of investigation is India healthcare's Electronic Health Record (EHR) with electronic patient journals in order to ensure appropriate security for accessing the appropriate resources and preventing unauthorized users from accessing.

8.0 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) Yip, W., Fu, H., Chen, A.T., Zhai, T., Jian, W., Xu, R., Pan, J., Hu, M., Zhou, Z., Chen, Q. and Mao, W., 2019. 10 years of health-care reform in China: progress and gaps in universal health coverage. *The Lancet*, *394*(10204), pp.1192-1204.
14) Baidoun, S.D., Salem, M.Z. and Omran, O.A., 2018. Assessment of TQM implementation level in Palestinian healthcare organizations: The case of Gaza Strip hospitals. *The TQM Journal*.
15) Abdellatif, A.A., Al-Marridi, A.Z., Mohamed, A., Erbad, A., Chiasserini, C.F. and Refaey, A., 2020. ssHealth: Toward secure, blockchain-enabled healthcare systems. *IEEE Network*, *34*(4), pp.312-319.
16) 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.
17) 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.
18) Hoffman, D.A., 2020. Increasing access to care: telehealth during COVID-19. *Journal of Law and the Biosciences*, *7*(1), p.lsaa043.

19) Esfahani, A.A., Ahmadi, H., Nilashi, M., Alizadeh, M., Bashiri, A., Farajzadeh, M.A., Shahmoradi, L., Nobakht, M. and Rasouli, H.R., 2018. An evaluation model for the implementation of hospital information system in public hospitals using multi-criteria-decision-making (MCDM) approaches. *International Journal of Engineering and Technology (UAE)*, *7*(1), pp.1-18.

20) Moro Visconti, R. and Morea, D., 2020. Healthcare digitalization and pay-for-performance incentives in smart hospital project financing. *International journal of environmental research and public health*, *17*(7), p.2318.

21) Enaizan, O., Zaidan, A.A., Alwi, N.M., Zaidan, B.B., Alsalem, M.A., Albahri, O.S. and Albahri, A.S., 2020. Electronic medical record systems: Decision support examination framework for individual, security and privacy concerns using multi-perspective analysis. *Health and Technology*, *10*(3), pp.795-822.

22) 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.