Journal of Administrative and Economic Sciences • Vol 17, Issue 2 (2024) • p 79-93

Challenges for Adopting Information Technology in Saudi Arabia's Healthcare: A Case Study

Mutiq Mohammed Almutiq

Department of Management Information Systems, College of Business and Economics, Qassim University, P.O. Box 6640, Buraidah 51452 • Kingdom of Saudi Arabia

mmatk@qu.edu.sa

Abstract:

This research is based on a case study conducted by means of observation at Al-Qassim National Hospital, Saudi Arabia. The findings of this case study have aided the exploration of the vision of Saudi Arabia's National Health Services (SA NHS) regarding the prioritization of information security in healthcare databases and the usage of information technology. The study observes the use of information technology and its practices and priorities regarding information security. This research gives a brief overview of Saudi Arabia's healthcare services. Moreover, different challenges including information security and successful adoption of information technology are discussed. As well, this work highlights some important drivers of the information security of electronic personal records (EPR). The paper presents the findings from this case study at Al-Qassim National Hospital.

Keywords: Information Technology, Healthcare, Information Security, Electronic Personal Records, Saudi Arabia.

1. Introduction

According to the World Health Organization (WHO), the concept of electronic health or eHealth means "unified usage for information technology and electronic communications in the health sector" [1]. Through its ambitious program, the Ministry of Health is striving to achieve the eHealth vision. Therefore, MOH aspires to considerable progress by implementing its eHealth strategies which were launched in 2011. There are two phases of implementation for these strategies, each lasting five years [1]. At present, patient records are scattered due to the absence of a unified system for patients' medical records. This has resulted in wasted resources and efforts, causing additional financial costs for the repeated treatment of patients for the same health issues by different healthcare providers [2, 3].

The goal of this study is to use a case study to investigate the impact of adopting information technology in Saudi Arabia's healthcare.

This research paper specifically attempts to empirically answer the following questions: Are there any challenges for adopting EPR technology in Saudi Arabia? If challenges exist, how can this research be utilized to analyze these challenges?

This study examines information security policies and procedures aiming to mitigate the existing threats in the healthcare organization's internal as well as external environment. The rest of the paper is organized as follows: A brief review of healthcare services in Saudi Arabia is presented in section 2. Challenges to the adoption of information technology in Saudi Arabia's healthcare system are discussed in section 3. Section 4 provides data of the basic drivers for information security of EPR. The case study is presented in section 5, and the main conclusions are stated in section 6.

2. Overview of Healthcare Services in Saudi Arabia

Directorate General for Health and Ambulance started its operations for providing healthcare facilities to the residents of Saudi Arabia in 1926. Later, in 1951, this became the Ministry of Health [4]. Delivering the highest-quality integrated and comprehensive healthcare services is the Ministry of Health's responsibility, and this includes establishing healthcare facilities throughout the nation with a hope of realizing their future vision [5]. According to Article 31 of The Basic Law of Saudi Arabia, "the State shall protect public health and provide healthcare to every citizen" [4]. In keeping with its mandate, the ministry is dedicated to providing healthcare at all levels, promoting overall health and preventing diseases, as well as creating the rules and legislations governing both the public and private health sectors. In addition, MOH is responsible for academic training in the area of health investment, as well as research activity and performance monitoring in healthcare facilities [6].

The Ministry of Health's vision and mission has become all the more important due to the country's 2.6% population growth rate from seven million in 1974 to thirty-five million in 2022. In total, 244 hospitals and 2037 **primary healthcare centres** are providing their services with the help of 240,000 employees belonging to 35 nationalities. Figure 1 shows that 8.7% of total government spending is dedicated to

healthcare services [7]. The per capita spending USD 482 is lower than that of many developed countries including USA, UK, Australia, and Germany whose spending is more than USD 2900 [8].

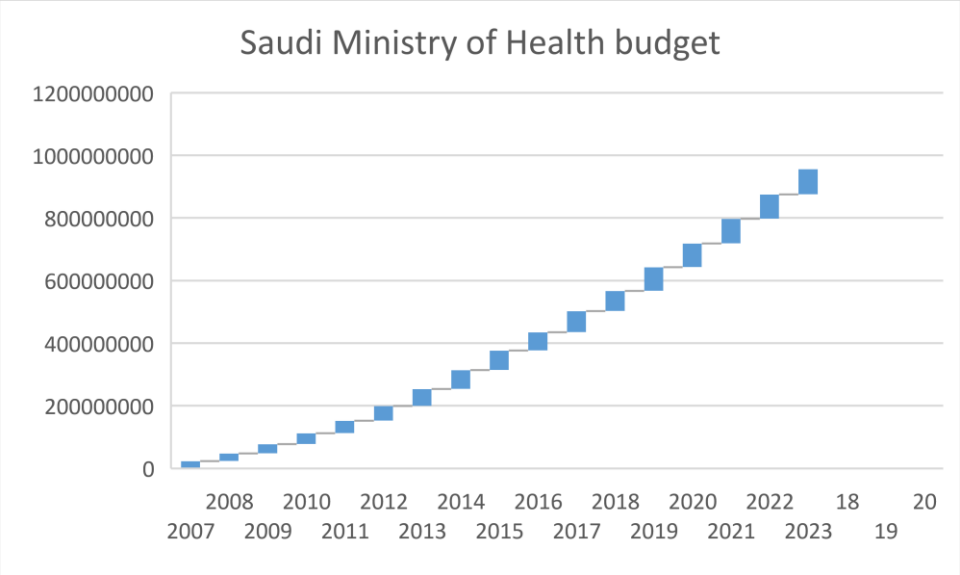

Figure 1: Saudi Ministry of Health budget

Some of the core values which the Ministry of Health endeavours to inculcate in the healthcare sector are that patient care comes first, followed by professionalism, justice, and quality [9].

The quality of healthcare in Saudi Arabia has improved significantly due to its driving factors, and this is being recognized both in the Middle Eastern region and worldwide [10]. During the last few decades, there has been a significant increase in state revenues due to increased oil production and the government displaying higher level of sensitivity towards improving the country's health services. Competent, qualified, and skilled manpower for the health sector has seen enormous growth, and people's level of awareness has increased due to health education [11]. All of these driving factors have helped Saudi Arabia to improve its healthcare services.

For improving the services of NHS, Saudi Arabia started its eHealth initiative in 2002. SA has a continuing plan to adopt information communication technologies for its institutions including healthcare services [12, 13]. The Ministry of Health foresees that the implementation of an eHealth strategy will help to save 10-15% of the public health budget. The Ministry invested USD 1.1 billion for the period 2008-2011 for the implementation of the eHealth strategy [4].

The eHealth strategy was adopted to enhance the quality of health services by reducing the waiting and processing times and the cost of delivery [3]. Therefore, enhancing the quality of services is the primary goal of information technology adoption.

Electronic personal records, which replaced the traditional paper-based records, were introduced by the Saudi government to improve the management of healthcare services

[10, 14]. The goals of this initiative were to decrease the amount of time patients had to wait, enable more efficient flow of patient information, and ensure the usage of clinical and non-clinical staff in the hospital in a more effective manner [15, 16]. Hence, the purpose of investing in eHealth is to provide therapeutic value and fulfil the demands of the healthcare workforce.

The eHealth strategy is a roadmap to cope with the challenges of program management, start and maintain the process of change at MOH, and mobilize service providers and staff. The MOH realizes that a comprehensive governance model coupled with clear guidelines are required to achieve the objectives of the strategy. Once implemented successfully, both MOH and the people of Saudi Arabia will benefit from this program [1, 17].

The MOH foresees the following benefits to patients if their eHealth vision is implemented successfully: Patients will have access to trustworthy health information via the internet, SMS, telephone, and pamphlets. There will be ease in finding convenient health services by using the internet. There will be a reduction in time and confusion while patients try to access services from various locations since previously recorded data will be made accessible to reputable providers and updated by the current services [17]. A quick and efficient diagnosis will be possible due to reduction in waiting time for services while avoiding unnecessary tests and procedures. There will be a reduction in the need for revisiting providers because of inaccurate information or scheduling problems [14, 17]. Patients will be able to check who else has viewed their information and for what reason at any moment, as well as view their own health information. They will have the option to add their own data, such as their current health, any symptoms, vital signs, or any other details pertaining to their providers.

Patients will also notice a difference in how MOH healthcare is delivered, as there is more confidence in healthcare professionals because they have access to the most recent training, skills, knowledge, capability, and competence while the healthcare professionals behaviour is still observed and evaluated [14, 17]. Patients will have faith that their personal health information is safeguarded from unwanted access and used only in accordance with their authorization [18]. People will be satisfied knowing that every service they use has sophisticated technology comparable to that found in industrialized nations. Knowing that their health information is accessible to providers through secure internet access with their permission and security keys in the event that they need medical attention when travelling within or outside of Saudi Arabia will provide them peace of mind [18]. Knowing that the MOH eHealth computer systems employed by the clinicians are able to reduce medical errors will increase their sense of security [18, 19].

The accomplishment of the eHealth vision will help healthcare providers since doctors, nurses, and other specialists will have simple access to patient data anywhere and at any time. They will have access to the best evidence-based information from reliable sources around the world. The clinical and administrative services needed by medical personnel will be available, including electronic recommendations [20]. With the help of teleconsultations and email, medical personnel will be able to contact their colleagues from anywhere in the world. Cutting-edge diagnostic equipment and

decision support services will be accessible [20]. Staff use of intelligent technology will help to avoid medical blunders and unfavourable outcomes. There will be access to services such as Continuous Medical Education (CME), which is largely available online. It will be possible to compare personal practice outcomes and trends to data on national performance. The employees' confidence will increase if they have access to the most advanced medical technology comparable to that used in other industrialized nations. [3, 19, 20].

Patients and healthcare professionals are not the only ones who will benefit from the use of information technology; with the success of the eHealth system, executives in hospitals, PHCs, regions, and corporate offices will also be able to manage efficiently thanks to the availability of all the data on a dashboard of up-to-date effectiveness markers, automatically recorded at the point of service and requiring no delays or manual processes to gather the data [20, 21]. The findings of diagnostic tests, as well as those of other patient consultations or services, will be sent electronically as soon as they are available so that healthcare personnel will not have to wait to learn the results [20, 21].

To identify issues, managers will also be able to delve deeply into the data that appears on the platform (e.g., by facility, area, supplier, etc.). It will be feasible to compare the performance of their area to that of other business areas. Additionally, comparative data from other nations will be available by the production of official reports [20, 21].

3. Challenges to the Adoption of Information Technology in Saudi Arabia's Healthcare

There are certain benefits to the adoption of information technology for healthcare services, but there are also significant limitations and challenges to its successful adoption.

3.1 Adoption of EPR is a Complex Task

Since healthcare services are complex and involve many factors, the management of EPR also becomes very complex, posing challenges to its successful implementation. There are numerous activities and processes involved in the delivery of healthcare services. According to Aldajani [16], one reason for the failure of information security in healthcare services is that the general clinical and managerial processes are underestimated by the health information systems. Another reason for difficulties in the adoption of information systems may be a conflict between the expectations of the system commissioner, producer, and end users [22]. Aldajani further argues that implementation of information systems in healthcare is a longer process than managerial change and corporate memory [16].

3.2 Standardization and Compatibility to Integrate the EPR

Aldajani [16] has observed that there are different products developed by different companies for different healthcare providers. Therefore, the EPRs being used in Saudi Arabia are based on different design, structure, and content [12]. This raises the issue of standardization and compatibility of EPRs for integrating records of different

healthcare providers. A sound plan for standardization will be required if SA NHS wishes to integrate the EPR of different healthcare providers.

3.3 Productivity Compared to Cost

Adoption of information systems is an expensive project because of the costs involved in hardware, software, and training of human resources [7, 23]. One of the purposes of implementing information systems is to enhance the productivity of the organization. However, during the initial stages, when staff are not well versed with the new system, there are risks that productivity may even decrease [22]. Therefore, it is also a challenge for healthcare providers to prepare their human resources for shifting to a new system of EPR.

3.4 EPR May Not Be According to Needs of Physicians

Generally, EPR does not give much freedom to physicians to express their ideas and opinions and the manner in which they may wish to organize a patient's medical information. Several researchers believe that this may constitute weaknesses in the design, structure, and content of the EPR [14, 15, 16, 22].

3.5 Resistance of Employees to Change

Generally, people feel comfortable using the traditional methods which have been in practice for a long time, showing resistance to change. Therefore, change in employee attitude, level of awareness, skills, and training should be considered by the SA Ministry of Health [14].

3.6 Access Rights of Patients

It is a challenge for healthcare providers to deal with the access rights of patients. With increased awareness, patients desire more access to and control over their EPRs. Patients may need to access their records to know about their health conditions and make plans and decisions [23]. However, shifting from paper-based traditional records to electronic personal records will also raise the question of who is responsible for the privacy of patient information [18]. By using EPRs, patients will lose their exclusive access to and control of their medical information [18].

3.7 Information Security

Information security of EPR is one of the biggest challenges for their successful implementation [18, 24, 25]. Use of EPR facilitates access to records at different locations which increases concerns about the security of information as high accessibility might result in unauthorized access and data theft [24]. Information security may be breached while the data is being transmitted from one place to other or by means of unauthorized access to information systems [18].

4. Basic Drivers of Information Security of EPR

Given the fact that information security remains a challenge in spite of all the progress in information security technology, the healthcare sector has to develop information security strategies that are enabled to cope with existing risks [26]. Plans to cope with

challenges posed by information security are affected by different drivers and factors of protection (shown in Figure 1).

The main driving factor of information security is to enhance and promote service quality in healthcare [27]. Safe handling and access to data in a secure manner helps to enhance the quality of the service. Aldajani [16] has highlighted three important issues related to enhancing the information security of an organization. First, there are technical issues with technology that can control access to information services. Second, there are organizational issues of resources, management, employees, and environment. Third, there are human issues of employee attitudes, skills, and level of competence that is compatible with the objectives of information security.

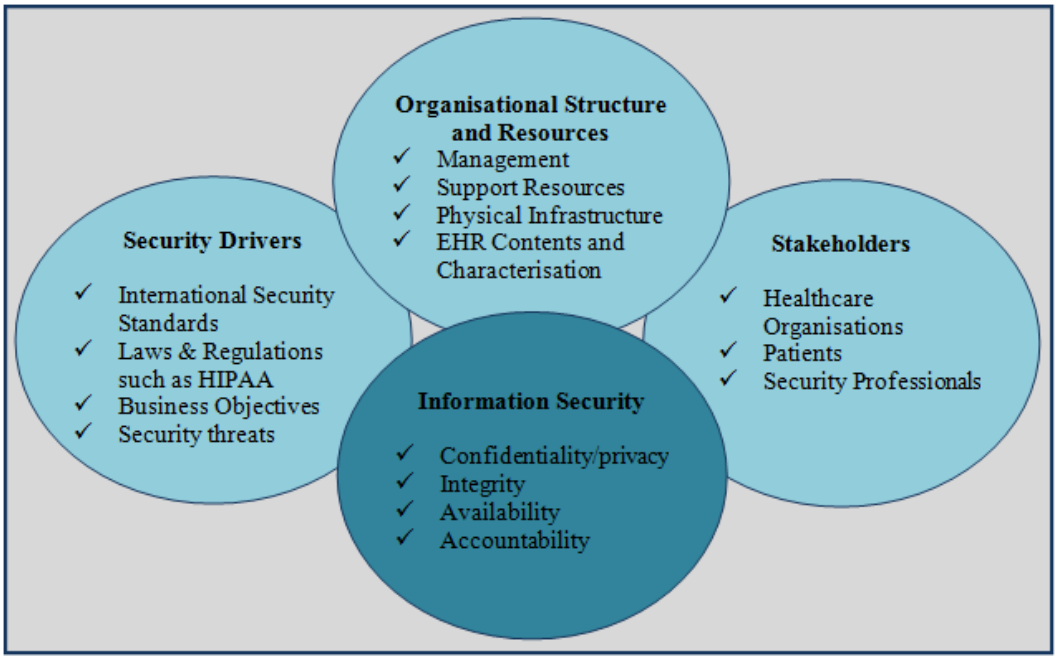

Figure 2: Information Security Requirements

4.1 Security Policies and Procedures

Security policies and procedures are aimed to guide all government agencies in Saudi Arabia in managing their security risks [28] through developing a framework which recognizes the fact that for a successful information security strategy, all three aspects (i.e., technical, organizational, and human) are important and need to be considered in detail. Saudi Arabia's Ministry of Health, as a government agency, is also responsible for adopting and implementing the recommendations of the framework [3]. It is also recommended by the framework that each government agency should develop its own information security strategy to cope with its unique challenges and requirements [18, 28].

The document admits that it will be impossible to develop a policy which addresses all the information security issues. Therefore, it is advised that a suit of policy documents be developed that covers all the important security areas [28]. Moreover, while developing an information security policy, various factors such as audience type and an

agency's business and size should be considered [25]. The specific threats that an organization encounters should be considered while developing an information security policy.

4.2 Objectives for Information Security Policy

An information security policy is aimed to define rules and expectations for the behaviour of management, security personnel, system administrators, and system users [26, 28, 29]. This policy permits security staff to keep track of, inquire about, and look into security incidents. It also defines consequences of violation, assists in compliance with laws and regulations, and minimizes the risk factors [26].

Information security policies should be developed to mitigate the existing threats in an organization's internal as well as external environment. The internal environment includes all the information interfaces where people of different departments inside the organization access the information systems. The external environment may include those external entities which interact on a regular basis with an organization such as customers, vendors, other government or private organizations, business process outsourcing providers, IT outsourcing providers, and the general public.

4.3 Classification of Information Security Policies

Research has shown that security policies are divided into two broad classes of common information security policies and specific information security policies [17, 22, 26, 24, 28, 29]. Policies for information security based on control groups and in accordance with international information security standards including ISO 27001 such as policies for access control, compliance, and business continuity are regarded as common policies [28]. Policies which are developed to meet the specific requirements of the information systems are called system-specific policies [26, 29]. Many studies suggest that three factors should be considered to assist the development of policies. First, a repository should be established that can be used as a model for developing both common and system-specific policies. Second, information security requirements of different organizations vary according to the significance of risks faced and the strength required for policies. Third, the policies have to be developed with a view to address a wide audience within an organization; therefore, the audience should be targeted to facilitate effective communication and implementation [26, 28, 29].

5. Case Study: Al-Qassim National Hospital, Saudi Arabia

This hospital is one of 415 healthcare providers in Saudi Arabia. The hospital started its operations on January 17th, 2009, and from its beginning has used information technology with the help of Digimedica, a software developed by American Digimedica Corporation to achieve improved clinical decision-making, better patient care, and enhanced documentation.

Clinical decision-making is facilitated by various tools ranging from diagnoses to prescriptions to recommendations for treatment plans. Moreover, doctors can also receive assistance from built-in medical dictionaries to be aware of adverse drug event alerts, dosage management, and generic drug recommendations.

EPRs used at the hospital allow for enhanced documentation as more than one user is allowed to access and update patient records simultaneously. This also results in comparatively more complete and accurate records. As compared to paper-based records, EPRs are more secure as their access can be controlled electronically. A security administration module incorporated in EPR software helps administrators to control access to patient information. Reporting capabilities are also enhanced as digital data can be easily manipulated. Comparative ease in manipulation of data helps to achieve useful research reports, drug recalls, statistics, and patient marketing.

Better clinical care of patients is facilitated by the modern features of EPR including the doctor's ability to access patient data from anywhere from the world. This enables web consultations over the internet.

Digimedica has the following medical modules that are used at the hospital to enter, process, and store medical information:

- Reservation
- Operating room
- ICU (Intensive Care Unit)
- IVF (In Vitro Fertilization)
- Blood Bank
- Outpatient
- Nurse stations
- NICU (Neonatal Intensive Care Unit)
- Lab
- Radiology
- Pharmacy
- Medical Records
- Emergency
- ADT (Androgen Deprivation Therapy for Cancer Treatment)
- Medical Reports

The hospital intends to achieve the following milestones by the application of information technology:

- Patient safety is increased by reducing errors in order transcriptions, improving legibility of orders, and increased availability of patient information.
- Better investigation strategies are possible due to improvised medical knowledge management.
- Electronic records save patients from being asked the same questions repeatedly, thus increasing the level of patient satisfaction.

- Level of satisfaction for medical staff is also increased due to effective automation providing a smooth and easy functional environment.
- Medical staff recruitment and retention is also improved.
- Communication is faster, more accurate, and less expensive.
- Time is saved due to instant access to medical records, shortened nursing handovers, and reduction of wait times for patients and staff [6].

5.1 Types of Data Stored in the Hospital Database

Information systems at the hospital are used to store and access patient data. The EPR contains the patient's personal information, such as their forename, surname, date of birth, national ID number, address, phone number, and next of kin. These personal details are required to identify and correspond with the patients. The second type of data which is stored in the EPR is the medical data.

The EPR also stores staff records electronically for management purposes. The staff record holds personal details of the staff member such as name, date of birth, national ID number, address, phone number, next of kin, employee number, designation, and date of joining.

Information systems are also used in the hospital to store information about financial accounts, inventory, receipts and bills, salaries and payments, and details of vendors.

5.2 Authorized Access to Patient's Data

Various personnel at the hospital are responsible for and authorized to use the information systems while storing or accessing patient data. Doctors, nurses, and support staff such as receptionists can enter and access the data. Patients can access the data only by request to the hospital, and access to data is granted in the form of hard copies of their reports and records.

5.3 EPR Access Control

Access to EPR is granted to staff and patients under certain conditions depending upon their role in the hospital. Doctors have full access to EPR to add information but not delete any existing data. Data once entered by a doctor cannot be modified by any other individual and cannot be deleted by the doctor him/herself after 24 hours. Therefore, any amendment to the medical information is possible only within 24 hours by the doctor who first entered the data. In the case of technical problems in the EPR system, doctors are authorized to maintain paper-based records; however, these records are not convenient for controlling unauthorized access.

It is not only doctors who have full access to EPR. The manager of the hospital and the staff of the information technology department also have full access to EPR. Data administrators are allowed to make changes to the existing records and update personal details such as change of address or telephone number, but they are not permitted to make any changes to the medical record. Personal details such as name, address, and phone number of the patient are available to all staff working at the hospital. Managers may need to access EPR for management purposes, but full access to records is not

necessary. Similarly, staff working for the information technology department must not be granted full access to EPR as this may result in information security breaches.

Hospital nurses have limited access to EPR as they are not enabled to access the complete personal details of the patients, previous medical history, previous medications, and information regarding history of allergies. However, nursing staff can access information about current recommended treatment, and they are authorized to enter monitoring information regarding temperature, blood pressure, and any test reports.

The pharmacists at the hospital can only read the EPR and do not have the right to make any revisions. Although Digimedica is enabled to integrate EPR with other hospitals and communicate with external partners, the hospital has avoided connecting with external partners including other hospitals. Only the information technology department can access information from outside the hospital, but all other staff have access from within. There is a maintenance agreement between the hospital and vendors of Digimedica. The software company is authorized to provide maintenance services externally. As part of the maintenance agreement, it is agreed that developers of Digimedica will ensure confidentiality of the hospital data. A program titled Team Viewer is in place for maintenance purposes. Under this program, a temporary password is created that can only be used once, and all activities under this temporary account can be monitored by the information technology department which is also enabled to stop the temporary account any time. The vendors are not authorized to remotely access the data by using the internet. The software company cannot ask for any statistics or details of records for the purpose of research.

Patients of the hospital are not authorized to access the EPR. Hard copies of their records can be provided to them on their personal request. Patient data can be accessed by a patient or his/her next of kin having proof of their relationship and authority to collect the information. Patients cannot control access to their electronic information. Patients' medical and personal details are recorded without the explicit and written consent of the patients. If people wish to hide their information from a particular person in the hospital for any reason, they are not enabled to do so. Since data is considered to be owned by the hospital and not by the patients, patients cannot ask to have their medical or personal data. As a matter of policy, patient data has to be deleted after five years. However, the hospital did not delete the data even after five years.

Data containing financial information of the hospital can only be accessed by the employees in the finance department. Medical and other staff are not authorized to access the financial information. The hospital's information technology department has access to financial information but cannot make changes to the data. Any changes can only be made by the finance department.

A username and password are used to access the EPR. All users are required to fill in an application form and sign it to access permission in order to get their username and password. The access permissions are controlled by the hospital manager and the information technology department. Hospital management are responsible for granting access rights and permission, whereas the information technology department ensures that access control is applied according to the decisions of the management.

5.4 Policy on Information Security

There is an information security policy for the hospital, and a copy of this policy is provided to the employees before signing their contract of employment. However, the policy is generic instead of being EPR specific. For example, it does not mention patient's consent and rights regarding EPR.

Management, in consultation with the information technology department, develops and implements the policies. Management is also responsible for reviewing the policies. Policies and procedures are revised with the changing requirements, and no periodic reviews are in practice. If an information security issue occurs elsewhere, this is communicated to the hospital. Then, the existing strategy is reviewed to strengthen the security against this reported issue.

The main instruments of information security are authentication of users by username and passwords and system of access rights and access control. Staff members are authorized to access the information on the basis of their role and responsibilities. Senior management makes decisions about granting access rights to different roles. The information technology department is responsible for ensuring the authorized access according to access rights as decided by management. If an employee leaves the hospital's employment, his/her username, password, and email account are deleted. However, staff are generally not asked or encouraged to change their passwords; this a potential risk.

All EPR users are provided with sufficient training to use the EPR, and this training includes information security perspectives. All employees (such as doctors or nurses) are required at the time of their recruitment to complete the training before starting their work. After successful completion of the training, their usernames and passwords are issued. Moreover, when there are changes in the software used at the hospital, staff are provided on-the-job training before the changes take place.

By restricting access to the internet, avoiding communication with external partners, and using an EPR that cannot be modified after 24 hours, the hospital has attempted to avoid information security risks. However, the existing strategy of information security does not address some important issues.

The medical and personal information of patients is disclosed upon request to third parties such as insurance companies; this is a sheer violation of patient privacy. This disclosure may also lead to further misuse of patient information.

Backup of databases is conducted on a daily basis, and two members of staff are assigned this job. However, the backup and original databases are housed in the same building, and there is a risk of data loss in the event of a natural disaster such as a fire or a flood, or in the event of a terrorist attack.

6 Conclusion

The hospital has used information technology since its inception. Although the hospital is not connected to external partners at present, it has a vision and will to do so in the near future. The hospital has benefitted from the use of EPR and is efficiently using

them to provide better services to their patients. There are several security features in place to safeguard the availability, confidentiality, and integrity of data. Information security, however, does not receive high consideration. A formal information security strategy is required to mitigate the existing risks. While there is a causal review system to update the policies, there is a need to develop a program of periodic reviews to minimize the effects of potential threats in the future. A perfect starting point for the hospital could be to adopt the guidelines which are given by the government.

Recommendations for future studies are to (a) measure the success of the health sector in applying electronic personal records (EPR); (b) analyze how confidential data can be secured; (c) determine the possibility of building an integrated health system that connects the beneficiaries of the private sector with each other and with the beneficiaries of the government sector; and (d) compare the results with other countries.

References

1. Ministry of Health e-Health Strategy (2013) " National e-Health Strategy " Online available at: http://www.moh.gov.sa/en/Ministry/nehs/Pages/Ehealth.aspx [Accessed 25 January 2023].
2. Altuwaijri, M. (2008) "Electronic-health in Saudi Arabia", Saudi Medical Journal, 29(2), p.p. 171-178
3. AlSadrah, Sana A. "Electronic medical records and health care promotion in Saudi Arabia: an overview." *Saudi medical journal* 41.6 (2020): 583.
4. Ministry of Health (2009) " Strategic Plan 2010-2019" Online available at: http://www.moh.gov.sa/Portal/WhatsNew/Documents/OKIstragi260p.pdf [Accessed 01 February 2023].
5. Ministry of Health vision (2014) " About the Ministry " Online available at: https://www.moh.gov.sa/en/Ministry/Statistics/book/Documents/Statistics-Book-1434.pdf [Accessed 16 January 2023].
6. Ministry of Health Mission (2014) " About the Ministry " Online available at: https://www.moh.gov.sa/en/Ministry/Statistics/book/Documents/1433.pdf [Accessed 16 January 2023].
7. Alhowaish, Abdulkarim K. "Healthcare spending and economic growth in Saudi Arabia: A Granger causality approach." *International Journal of Scientific & Engineering Research* 5.1 (2014): 1471-1476.
8. Springmann M, Mason-D'Croz D, Robinson S, Wiebe K, Godfray HCJ, et al. (2018) Health-motivated taxes on red and processed meat: A modelling study on optimal tax levels and associated health impacts. PLOS ONE 13(11): e0204139. https://doi.org/10.1371/journal.pone.0204139
9. Ministry of Health Values (2014) " About the Ministry " Online available at: http://www.moh.gov.sa/en/Ministry/About/Pages/Values.aspx [Accessed 16 January 2023].

10. ElGibreen, Hebah. "Chapter 5: Health transformation in Saudi Arabia via connected health technologies." *Technology and Global Public Health* (2020): 83-99.

11. Househ, M., Al-Tuwaijri, M., Al-Dosari, B. (2010), "Establishing an Electronic Health Centre of Research Excellence (E-CoRE) within the Kingdom of Saudi Arabia", Health San Francisco, 4(1), p.p. 42-46

12. Aljohani, Nasser, and Daniel Chandran. "Adoption of M-Health Applications: The Saudi Arabian Healthcare Perspectives." (2019).

13. Hokroh, Mohammed, Gill Green, and Mochamad Soleton. "Factors influencing health wearables adoption and usage in Saudi Arabia." *Journal of Management and Economic Studies* 2.2 (2020): 89-98.

14. Alshahrani, Abdullah, Derek Stewart, and Katie MacLure. "A systematic review of the adoption and acceptance of eHealth in Saudi Arabia: Views of multiple stakeholders." *International journal of medical informatics* 128 (2019): 7-17

15. Rasmi, Mohammad, et al. "Healthcare professionals' acceptance Electronic Health Records system: Critical literature review (Jordan case study)." *International Journal of Healthcare Management* 13.sup1 (2020): 48-60

16. M. Aldajani, "Electronic Patient Record Security Policy in Saudi Arabia National Health Services," PhD thesis, De Montfort University, February 2012.

17. Alassafi, Madini O. "Success indicators for an efficient utilization of cloud computing in healthcare organizations: Saudi healthcare as case study." *Computer Methods and Programs in Biomedicine* 212 (2021): 106466

18. Almaghrabi, Nada Saddig, and Bussma Ahmed Bugis. "Patient Confidentiality of Electronic Health Records: A Recent Review of the Saudi Literature." *Dr. Sulaiman Al Habib Medical Journal* 4.3 (2022): 126-135.

19. Benefits to Patients (2011) " National e-Health Strategy " Online available at: http://www.moh.gov.sa/en/Ministry/nehs/Pages/Benefits-to-Patients.aspx [Accessed 29 January 2023].

20. Taitsman JK, VanLandingham A, Grimm CA. Commercial influences on electronic health records and adverse effects on clinical decision-making. JAMA Int Med. 2020;180(7):925

21. Benefits to Health System Managers (2011) " National e-Health Strategy " Online available at: http://www.moh.gov.sa/en/Ministry/nehs/Pages/Benefits-to-Health-System-Managers.aspx [Accessed 29 January 2023].

22. Arabi, Yaseen M., et al. "Electronic medical record implementation in a large healthcare system from a leadership perspective." *BMC Medical Informatics and Decision Making* 22.1 (2022): 1-10.

23. Ajagbe, Sunday Adeola, and Ademola O. Adesina. "Design and development of an access control based electronic medical record (EMR)." *CPJ* 2020008 (2020): 26108.

24. Phichitchaisopa, Nisakorn, and Thanakorn Naenna. “Factors affecting the adoption of healthcare information technology.” *EXCLI journal* 12 (2013): 413.

25. Alanezi, Fahad. “Factors affecting the adoption of e-health system in the Kingdom of Saudi Arabia.” *International Health* 13.5 (2021): 456-470.

26. Almutiq, Mutiq Mohammed. *An evaluation model for information security strategies in healthcare data systems*. Diss. Keele University, 2018.

27. Ayanlade, Oluwatoyin Seun. “Electronic Medical Record System as a central ICT tool for quality healthcare services: Nigeria as a case study.” *African Journal of Science, Technology, Innovation and Development* 10.2 (2018): 147-157.

28. Computer Emergency Response Team (2011) “ Information Security Strategy Policies and Procedures Development Framework for Government Agencies “ Communication and Information Technology Commission 2011.

29. Negi, Lokesh, and Shobha Bhatt. “Framework for securing EPR records with Searchable encryption & AES.” *2022 IEEE Delhi Section Conference (DELCON)*. IEEE, 2022.