Journal of Theoretical and Applied Information Technology
31st January 2023. Vol.101. No 2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

EXAMINING THE FACTORS FOR NON-COMPLIANCE OF SAUDI HEALTH ORGANIZATIONS FOR E-HEALTH SECURITY AND PRIVACY

KHALIL IBRAHIM ALMUWAIL[1] , ABDULAZIZ SAAD ALBARRAK [1], MUHAMMAD NASIR MUMTAZ BHUTTA[2], HEIDER A. M. WAHSHEH[1]

[1]Department of Information Systems, College of Computer Science and Information Technology, King Faisal University, P.O. Box 400, Al-Ahsa 31982, Saudi Arabia

[2]Computer Science and Information Technology Dept, College of Engineering, Abu Dhabi University, Abu Dhabi, United Arab Emirates

E-mail: [1]hwahsheh@kfu.edu.sa
E-mail: [1]heiderwahsheh@gmail.com

ABSTRACT

Recently, there has been increasing concern about the security of patient data and the impact of Saudi health organizations' non-compliance with privacy and electronic health security regulations. However, there is a limited number of studies related to security compliances in Saudi healthcare organizations. This research aims to study the challenges of security compliance standards in hospitals for patient data security and privacy in the Saudi Arabian healthcare sector. Healthcare facilities of all sizes need help in maintaining security rule compliance. Analysis of factors influencing complete adherence to security rule compliance has begun as part of the non-compliance study. Various theoretical frameworks and conceptual models have been used in previous studies to help small and medium healthcare facilities comply with security compliance successfully. In addition, there is a demand to utilize security compliance frameworks in hospitals, and national security standards are essential for protecting patient data. Therefore, this study intends to investigate the factors that lead to non-compliance with E-Health security and privacy in Saudi health organizations. A set of hypotheses were developed to achieve the study's goal.

Furthermore, the study follows a quantitative approach to evaluate the proposed model and hypotheses. Statistical Package for Social Sciences (SPSS) is employed to analyze the users' responses, and the IBM analysis of moment structures (AMOS) is used to validate the research model. The findings suggest that understanding management support, security awareness, security culture, and computer self-efficacy is essential to ensure compliance with the security rules.

Keywords: *Security compliance, E-health security, data privacy, data protection, security non-compliance*

1. INTRODUCTION

Numerous countries are currently struggling to provide their people with high-quality, affordable healthcare. Today, the Ministry of Health and other government-run health institutions offer free healthcare to all Saudis and foreigners working in Saudi Arabia's public sector, including the military. The government demands that their employers' health insurance plans cover foreign nationals working in the private sector. Adopting health information systems (HISs) may have various advantages, including better patient care, fewer medical mistakes, and easier access to data. A robust security architecture is required for a dependable and coherent information system (IS) (i.e., confidentiality, integrity, and availability). Another essential component in preserving data security and policy compliance is employee attitude. The only problem is that you have no control over it. An insider danger arises when activities are misused, such as when authorities are abused or policies are not followed. Internal threats are more harmful than external threats because workers are aware of the security guidelines in their firm. As a result, firms often implement Information security (IS) policies to raise employee understanding of the need to adhere

to information security compliance standards (ISCB) [1].

The Saudi government has dramatically focused on developing primary, secondary, and tertiary healthcare services [2]. Due to this development, Saudi Arabia's health has improved dramatically in recent decades. Many issues confront the Saudi healthcare system, such as a lack of Saudi healthcare workers, the ministry's multiple responsibilities, limited financial funds, shifting disease patterns and limited availability of free services, the absence of a national emergency implementation plan, poor accessibility to some healthcare facilities, a lack of a national health information system and the inefficiencies of e-health strategy's opportunities [2]. The Ministry of Health (MOH) and other relevant sectors should focus their efforts on adopting and guaranteeing the implementation of the new healthcare strategy to solve these issues and continue enhancing the status of the Saudi healthcare system. A growing volume of information presents a difficult challenge for healthcare. More resources are needed to keep up with the increasing demand for healthcare in the future because of the ever-increasing amount of information available. As a result, cloud computing must be practical as a support. The healthcare industry believes that cloud computing can help to improve patient data security and privacy [3].

With the Global Health Security Agenda (GHSA) and Sustainable Development Goals (SDGs) in consideration, the Saudi Arabian government's commitment to these initiatives is consistent with the strategic direction of the Saudi Vision 2030 [4]. To assist academics, policymakers, and professionals plan, it is critical to conduct a study and publish findings that focus on enhancing the population's quality of life and well-being. Health in All Policies (HiAP) and the Model of Care focus on patient-centered healthcare in the National Transformation Program, Saudi Vision 2030 [4]. This means that data may be used to map and model population health requirements and comprehend the dynamic of socioeconomic determinants of health. As a result, a healthcare reform implementation strategy that satisfies the population's needs is critical to improving overall health and quality of life [5].

Saudi Arabia faces many challenges in implementing e-Health for data security, including cultural, administrative, and human resource concerns [6]. Several previous studies indicated some of the obstacles associated with procurement issues and its implications for the hospital's patient welfare, such as the possibility that a disorderly procurement plan might result in systems being unable to communicate with one another [6] and [7].

1.1 Need for the study

New security threats and breaches have arisen due to the increased use of mobile computers [8]. According to [9], healthcare organizations are more likely to deal with security issues after the fact pointed out that while adopting new products and services, these firms do not always consider security. Furthermore, computer security is often incorporated as a last-minute addition to the system [9]. As a result of the strict HIPAA laws that focus primarily on administrative security measures, healthcare businesses have taken a more technical approach to dealing with security concerns. There is a lack of security awareness among Saudi healthcare employees [9]. In addition, there is a demand for the training program to empower security and privacy knowledge among healthcare workers. Factors of Non-compliance of Saudi health organizations for e-Health security and privacy were not thoroughly examined [10].

This study aims to identify the factors inhibiting Saudi health organizations from properly adopting the security compliance frameworks and Saudi national security guide for the e-Health sector and formulating a model to guide health organizations to implement compliance frameworks properly. This research aims to answer the questions: (1) What are the factors influencing the implementation of compliance standards in Saudi healthcare centers? (2) How to design a framework to achieve security compliance in Saudi healthcare centers?

1.2 Paper Structure

The structure of this paper is as follows. Section 2 presents the literature review. Section 3 discusses the research design, and section 4 illustrates our research methodology. Section 5 explores the data collection and analysis. Section 6 discusses the obtained results, and section 7 draws the concluding remarks and future work.

2. LITERATURE REVIEW

Saudi Arabia has a national healthcare system in which the government offers free healthcare services through various government institutions [4]. In addition, the private sector is playing an increasingly important role and increasing its involvement in delivering healthcare services. Saudi Arabia offers finance and provides primary, secondary, and tertiary care to certain enrolled security and armed

services populations: The Ministry of Defense and Aviation, the Ministry of Interior, and the Saudi Arabian National Guard, to name a few examples [4]. Recently, particularly during the COVID-19 pandemic, there has been a growing attraction to utilizing secure techniques in healthcare systems, improving workflow, decreasing costs, and growing the flexibility of providing healthcare benefits to users [7]. As a result of these agencies, the kingdom also has several other government agencies responsible for delivering and financing healthcare services [11].

The Ministry of Labor and Social Affairs oversees institutions for the mentally ill and orphan care homes. Medical services are available to guests at these establishments. Some of the people it serves receive healthcare through the General Presidency of Youth Welfare and the General Organization for Social Insurance and Insurance [4]. The Royal Commission serves people in the industrial cities of Jubail and Yanbu for Jubail and Yanbu. For the sake of its employees, Saudi Arabian Airlines has its healthcare facilities. Numerous medical colleges and hospitals in the Kingdom provide specialized medical services and educational programs in addition to conducting health research with other institutions [4].

The healthcare system's effectiveness as a whole depends on the effectiveness of hospitals, which are major users of health resources. To put it another way, cloud computing in healthcare refers to storing, managing, and processing patient data on remote servers that can be accessed online [11. Using cloud storage, healthcare practitioners and hospitals can store massive volumes of data in a secure environment maintained by IT professionals in a network of remotely accessible computers [5]. Because of the EMR mandate, healthcare organizations all throughout the Kingdom have turned to the internet to store and safeguard patient data [11]. Collaborative patient care in the United States is now easier due to cloud storage for electronic medical information. Doctors can more easily see or share a patient's medical records when they are stored in the cloud [11].

Healthcare organizations must develop a security plan that guarantees compliance while securing patient data. Achieving this purpose will result in a very successful information security policy for healthcare. However, many organizations have concentrated on establishing basic technical processes rather than adopting strategic solutions [12]. The three areas of focus for compliance at private hospitals were patient care, regulatory compliance, and human resource management. Due to the complexity of relevant law and the fact that it is constantly changing, many hospitals need help to ensure compliance [13]. Private hospitals are subject to the risk of compliance. It was decided to create a compliance framework to minimize the risk of private hospitals in South Africa compliance. Outsourcing may be explored to reduce compliance costs while focusing on the company's performance [13].

Seriously, e-health technology has been employed in Saudi Arabia's healthcare institutions to improve the quality and accessibility of healthcare services [14]. The government controls the country's healthcare system, which provides medical services via several government organizations. Saudi Arabia is rated 26th in the world for the quality of its healthcare services. Saudi Arabians are very anxious about the appropriate usage of electronic health facilities. E-health and electronic information systems have already started to be implemented in several hospitals and organizations. Even so, among MOH entities, e-health service adoption is slowly growing [15].

From three different stakeholder perspectives, E-health barriers in Saudi Arabia have been studied and categorized by [16]. People and healthcare professionals in KSA blamed the failure of e-health on a lack of connectivity among hospital information systems (HISs). At the same time, IT specialists identified public health security as the most significant barrier [16]. Regarding health, e-health gives patients more power since it allows them to exchange data with healthcare experts [14] and [17]. By using telemedicine, e-health is making healthcare services more accessible and affordable for patients. It also makes Saudi Arabia's public health management more reliable [15]

3. RESEARCH DESIGN

3.1 Research Model and Hypotheses

Saudi Arabia has pinpointed the advantages of e-health and health information management in providing healthcare services. Government makes every effort to ensure that the technology is widely adopted. For instance, in Saudi Arabia, computerized provider order entry (CPOE), clinical decision support systems (CDSS), electronic medical records (EMR), and electronic health records (EHR) are improving healthcare professional-patient interactions and expanding patient access to health data [18].

3.1.1 Management Support

Management support (MS) has been highlighted in previous studies as a critical reoccurring factor in system performance. According to [19], the literature on Information Systems (IS) has long acknowledged the significance of top-level management support (TMS). Leadership's commitment to organizational transformation is essential for its eventual success. When a senior management project sponsors/champions, the CEO and other senior managers commit time to review plans, follow up on results, and enable management problems (TMS). According to the authors, TMS is necessary in all cases and offers a convincing explanation for why specific initiatives were successful and others were not. Various critical success factors (CSFs) are essential for project success, but the most important one is TMS, according to [19].

The study of [20] examined how electronic health records are used in government hospitals. An online questionnaire was adopted for data collection; only three government hospitals (15.8%) reported using EHRs. EHR implementation in hospitals was difficult for certain IT managers. Some doctors and nurses refused to utilize EHRs cooperatively. Saudi Arabian healthcare information specialists [21] examined the role of e-Health in the Kingdom of Saudi Arabia. Participants' data were analyzed using a case study approach and conceptual analysis, including interviews conducted with nine prominent Saudi Arabian healthcare staff. According to the findings, there were differences in adopting e-Health across Saudi healthcare centers. It was suggested that a different Saudi e-Health organization be established and a coherent policy be developed for implementing Saudi e-health programs [21].

H1- There is a significant positive relationship between management support and security compliance.

3.1.2 Security Behavior

The study of [22] conducted five interviews with the IT directors responsible for hospital EMR systems using a semi-structured interview as the study instrument. They discovered that EMRs in Hebron are woefully underequipped. In addition, they observed that the public hospital in Hebron is better at using EMRs than the private ones. It is recommended that hospitals in Palestine increase their EMR system investments to improve their capabilities. There is a need for the Palestinian Ministry of Health and the Palestinian government to support hospitals in their efforts [22].

Authors [23] conducted a study to determine the competitiveness of the EHR vendor market in the United States (US) and the degree to which individual Medicare beneficiaries' medical records are fragmented across the many EHR vendors available in the US healthcare system. Our research shows that the EHR vendor market was competitive in 2016 but is on the verge of becoming highly concentrated. Patients' medical records were also highly dispersed, with only 4.5 percent of expenditure-weighted individual Medicare beneficiaries having their MU medical records associated with one vendor. In comparison, 19.8 percent of expenditure-weighted beneficiaries stored their MU medical records in eight or more vendors. Interoperability issues among multiple EHR vendors could make it to transfer medical records between different providers, reducing the advantages of competition among vendors. This emphasized the necessity of continuing present attempts toward interoperability in the future.

H2- There is a significant positive relationship between security behavior and security compliance.

3.1.3 Security Awareness

The study of [24] based their model on various dimensions, including employees' awareness of and contentment with information security, assessing its utility, fairness, quality, self-efficacy, and specific organizational characteristics. Results demonstrated that awareness, perceived quality, and self-efficacy significantly influenced employees' ISCB. The study of [25] built their model on a range of areas, including employees' awareness of and contentment with information security, assessment of its utility, fairness, and quality, self-efficacy, and specific organizational characteristics. The results also demonstrated that awareness, perceived quality, and self-efficacy strongly influenced employees' ISCB.

Authors in [26] analyzed the discharge data from the Medicare Patient Safety Monitoring System (PSMS) for 2012 and 2013. One of the three diseases studied was an acute cardiovascular illness, pneumonia, or a condition that necessitated surgery. The primary outcome measures were in-hospital adverse events, including hospital-acquired infections, adverse drug events (based on selected drugs), general events, and post-procedure events. Chart abstraction was used to evaluate rates of adverse events and patient exposure to an electronic EHR. The study's outcome revealed that EHR reduced the risk of in-hospital complications for patients with cardiovascular, pneumonia, and surgical conditions.

The study of [27] conducted a cross-sectional survey in Dhaka, Bangladesh's capital city, to gather data from 300 participants in several private and public hospitals. The partial least squares (PLS) method used an SEM-based statistical analysis methodology to examine the collected data. By implementing social tactics to encourage physicians to utilize the EHR system, assuring technical sufficiency, and training to promote EHR system use, the findings imply that policymakers should work to encourage greater adoption of the electronic health record system. Additional considerations include finding doctors willing to try new information technologies and removing obstacles like computer crashes, bad infrastructure with inconsistent power supply, and other issues [27].

H3- There is a significant positive relationship between security awareness and security compliance.

3.1.4 Security Effectiveness

The study of [11] requested EHR stakeholders in a large-scale healthcare organization to complete a survey questionnaire that used original and modified concepts from a Consolidated Framework for Implementation Research (CFIR) to identify barriers and opportunities for engagement. An in-depth analysis of the findings led to recommendations on the usefulness of engagement process modeling and a discussion of intervention opportunities that might be employed to alleviate engagement barriers [11]. The results suggested that all parameters except understanding a physical system affected information security awareness [24]. Furthermore, they used two theories, protection motivation theory (PMT) and GDT, to establish parameters connected to ISCB. The domains tested through the PMT were perceived threat vulnerability, threat severity, reaction efficacy, and security effectiveness. Factors examined by the GDT included punishment certainty and severity. Security effectiveness was the only significant predictor of ISCB compared to the other variables.

Dental healthcare professionals were asked to complete a questionnaire about the demographic trends, security, and effectiveness of their electronic health record systems (EHRs). Participants came from five different areas of Saudi Arabia, comprising 270 people. Concerns about privacy, staff compliance, and expenses have influenced healthcare professionals' views on Electronic Health Records [28].

The study of [29] performed a cross-sectional analysis of 371 health systems' EHR metadata. They indicated that US doctors spent more time a day actively using the EHR, received more system-generated messages, wrote a higher proportion of automatically generated note text and used the EHR more after-hours than non-US clinicians. Results of this study reveal that US physicians, compared to non-US clinicians, have a higher EHR burden. This burden might be reduced by eliminating EHR uncertainty and streamlining documentation requirements.

H4- There is a significant positive relationship between security effectiveness and security compliance

Based on the variables, a set of hypotheses is developed as presented in table 1. A sum of four hypotheses is designed to investigate the non – compliance of security and privacy standards in Saudi healthcare centers.

Table 1: Hypotheses.

H1- There is a significant positive relationship between management support and security compliance
H2- There is a significant positive relationship between security behavior and security compliance
H3- There is a significant positive relationship between security awareness and security compliance
H4- There is a significant positive relationship between security effectiveness and security compliance

3.2 Theoretical Framework

This research will propose and test a model of the elements that may impact and lead to Security compliance to understand the determinants. Several theories will be incorporated into this investigation. Human behavior can be better understood and predicted using the theory of reasoned action (TRA). On the other hand, TRA was proven ineffective in predicting behavior when users thought they had little control over their actions. When [30] contributed the missing dimension to the theory of planned behavior, he called it "perceived behavioral control" (TPB). According to [31], the concept of perceived self-efficacy is congruent with the perceived behavioral control component of the theory of planned behavior model. In the social cognitive theory [32], self-efficacy is a concept that describes an individual's belief that they are capable of completing a task.

The theory of planned action is an extension of the rational action theory. In situations when individuals sensed little volitional control over their actions, the theory of planned behavior could overcome the constraints of the theory of rational action [32]. It was characterized by [32] as the antecedent construct in the theory of planned behavior (TPB). An attitude is a subjective judgment of how you feel about particular conduct; subjective standards are your beliefs of what society expects of you; and perceived behavioral control is how much control you believe you have over your actions. The Protection Motivation Theory (PMT) is an expectancy theory in which there is a belief that a behavior will lead to an expected outcome [20]. The protection motive is important in forecasting how an act of compliance can negatively affect compliance intention by introducing unforeseen hazards imposed by the act of compliance. Fear drives action.

Based on the study [31], the factors such as management support, security behavior, security awareness, security effectiveness, and security compliance are selected as dependent and independent variables. Figure 1 represents the conceptual framework of the proposed study.

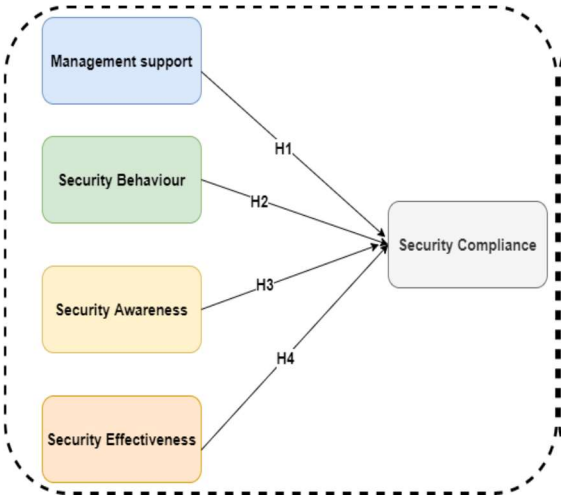

Figure 1: Conceptual framework

4. RESEARCH METHODOLOGY

The goal of quantitative research is to investigate the statistical significance of the correlations between variables in the study. Using an online questionnaire, we can identify the most significant intrinsic elements that influence a user's perception on security compliance in Saudi Arabia. Google Forms is typically used to distribute this study's questionnaire. Participants may interact anonymously, swiftly, and efficiently using a Google form while simultaneously collecting data. It will also be made available to the general public via social media. On a Likert scale of 1 to 5, participants rate how strongly they agree or disagree with each measurement. The research model and hypothesis are derived from the literature review by obtaining up-to-date research articles from Saudi digital libraries relevant to this study's subject matter.

Exploratory research is commonly used to illuminate previously unstudied or esoteric topics. In the end, explorative research's versatility is obvious; it can be undertaken through literary quests, inquiries into certain topics' experiences, or case studies. The purpose of experiments is to shed light on circumstances too complex to be well addressed in academic literature. Deductive reasoning is used to investigate the security and privacy practices KSA healthcare organizations employ. Allowing regular or important interrelationships with raw data is a primary goal of inductive reasoning. To reach the study's objective, this strategy focuses on organization behavior towards E-Health. Deductive reasoning begins with an interpretation of the text and ends with several vital concepts, as mentioned in [33].

Statistical Tools and techniques are also used in this study. To determine if the model's internal consistency may be relied upon as a reliable performance indicator. Between 0 and 1, the Cronbach's alpha scale measures the reliability of a test. The value closest to one suggests good consistency, whereas the acceptable dependability rate is 0.7, and the value closest to one implies outstanding reliability. In addition, exploratory research is appropriate when reliability ratings are between 0.6 and 0.7. Statistical Package for Social Sciences (IBM SPSS) was used to determine Cronbach's alpha.

4.1 Population and Sampling

The population for the study will be the healthcare employees in Saudi Healthcare facilities. The researcher is part of the healthcare professionals. The only option to get to all Saudi Arabians is to sample users randomly. Data can be analyzed using a combination of these methods, which are not mutually exclusive and can work well together. This study will use a quantitative technique to make conclusions on healthcare organizations' use of E-Health [32].

4.2 Structured Equation Modeling

Multiple regression and factor analysis techniques are combined in Structural Equations Modeling (SEM) to allow researchers to simultaneously explore many interconnected dependent connections between the measured variables and the latent constructs. Predictive modeling may be improved by using SEM to assess research data and produce an accurate estimate. It is also possible to test the constructs' unidimensionality, reliability, validity, and fitness using SEM and Confirmatory Factor Analysis (CFA). In addition, SEM may do a Multiple Regression Analysis on the given model and study hypothesis.

4.3 Confirmatory Factor Analysis

Confirmatory Factor Analysis is a method for determining how well the measured variables represent a reduced number of constructs. CFA assesses the accuracy of a model's input data by comparing it to the measured data. Measures such as fit quality, correlation, and other model properties may be examined using CFA to determine whether the model itself is valid. The goal of CFA is to discover latent variables that explain the variance and covariation among a collection of indicators. While CFA is part of the structural equation modeling (SEM) framework, the CFA method is also used to examine measurement models' validity and test hypotheses in structural models.

4.4 Multiple Regression Analysis

Modeling relationships between continuous response variables and continuous or categorical explanatory factors using multiple linear regression is more complex than modeling relationships between one continuous response variable and one continuous or categorical explanatory variable. Response and predictor variables may be referred to by other names in different contexts [34].

4.5 Goodness of Fit Measures

GOF metrics refer to how well the provided model reproduces the observed covariance matrix among the indicator items. GOF's evaluation of the research model's goodness of fit (GOF) can accurately predict research findings. To get a sense of how well your model fits the data, there are five standard metrics: the Comparative Fit Index, the Adjusted Fit Index, the Root Mean Square Error of Approximation (RMSEA), Tucker-Lewis index, and Chi Square / Degrees of Freedom (Chisq/df) [35]. Confirmatory Factor Analysis (CFA) and structural model goodness of fit metrics will be presented (Multiple Regression Analysis). (CFI) is less affected by the model's level of complexity. (CFI) must have a rate greater than or equal to 0.9. As long as (AGFI) is bigger than 0.8the rate of 0.9 is also acceptable (TLI). Indices that measure how well you fit a data set incrementally include CFI, AGFI, and TLI. Regarding the absolute fit index (RMSEA), the optimum value ranges from 0.05 to 0.08. (RMSEA) (Chisq/df) is one of the fit categories that should have a value less than 5.0. Table 2 provides an overview of the suggested GOF model metrics [35]. If the chosen indices are not increasing reasonably, then the model will need to be refined.

Table 2: Acceptable Model Fit.

Category	Index	Level of acceptance
Incremental fit	CFI	The value > 0.9
	TLI	The value > 0.9
	AGFI	The value > 0.8
	GFI	The value > 0.9
The absolute fit	RMSEA	0.05 ≤value ≥ 0.08
The parsimonious fit	Chisq / df	The value < 5

5. DATA COLLECTION AND ANALYSIS

The study questionnaire was used to gather the data. Statistical software packages such as SPSS and Analysis of Moment Structures (AMOS) were used to validate the model and study assumptions. Based on this research's evaluation of the produced model, it is examined for its unidimensionality, tested for its fit to the observed variables, and evaluated for its validity and reliability of the model's components. The Structural Equation Modeling (SEM) approach was used to assess the study model and assumptions. The questionnaire was updated according to the participants' responses. The Cronbach's Alpha is also increased for the questionnaire.

Upon completion of the pilot study and reconstruction of the questionnaire, the new questionnaire was re-uploaded online and the survey questionnaire was distributed again. According to standards, 208 completed responses were received, which is considered an acceptable response rate

[35]. The minimum allowable response rate for a survey is 100 (see table 3).

Table 3: Construct Reliability

Construct	Cronbach's Alpha
Management support	0.80
Security Behavior	0.70
Security Awareness	0.93
Security Effectiveness	0.88
Security Compliance	0.83

5.1 Assessment of the Measurement Model

It was decided to do a Confirmatory Factor Analysis (CFA) to assess the measurement model and its components. It is a statistical approach for evaluating the data's suitability for use in a measurement model that has been proposed. CFA and IBM AMOS were used to test the measurement model's validity. It was tested using three metrics: unidimensionality, model fit, construct validity and dependability. Figure 2 presents the measurement model of the proposed study in IBM AMOS. It contains the independent variables include Management support (Mg), Security Behavior (SB), Security Awareness (SA), Security Effectiveness (SE), and the dependent variable, Security Compliance (SC).

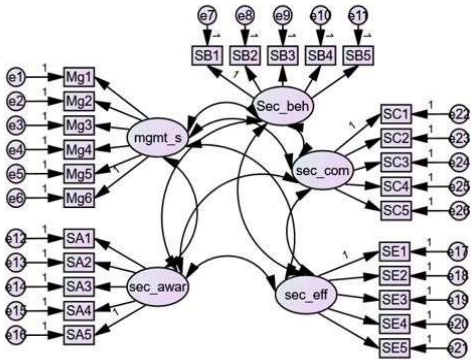

Figure 2: The measurement model in IBM AMOS

5.2 Unidimensionality and Goodness of Fit Measures (GOF)

To examine the connections between the model's measured variables and their underlying dimensions, the concept of unidimensionality was employed. A single underlying dimension must be linked to each model's measured variable [36].

Table 4 displays the findings of the 26 items' confirmatory factor analysis based on the data obtained. No measurements met their recommendations except for the RMSEA, which was close to the desired value.

Table 4: The Model Fit results

GOF	GFI	AGFI	RMSEA	CFI	TLI	Chisq /df
The measurement model	0.837	0.770	0.09	0.944	0.929	2.423

The study of [35] suggested removing any measured variable with a low communality value to improve the model's overall goodness of fit. Table 5 below shows that all measurements in the updated model met the acceptable value.

Table 5: The Model Fit results.

GOF	GFI	AGFI	RMSEA	CFI	TLI	Chisq /df
The measurement model	0.924	0.878	0.085	0.944	0.929	1.752

Model internal consistency is measured to determine the model's trustworthiness [37]. Model constructs are tested for reliability using the Cronbach's Alpha metric. Cronbach's alpha should be at least 0.7. Table 6 shows the refined construct reliability. It shows that Cronbach's Alpha for all variables is more than 0.80.

Table 6: Refined Construct Reliability

Construct	Cronbach's Alpha
Management support	0.92
Security Behavior	0.81
Security Awareness	0.94
Security Effectiveness	0.92
Security Compliance	0.95

5.3 Structural Equation Modeling

The model and research hypotheses were built using structural equations modeling. Various regression and factors analysis are combined to examine multiple linked dependencies between the constructs and the measured variables [35]. After completing the refinement steps, the refined model is shown in Figure 3.

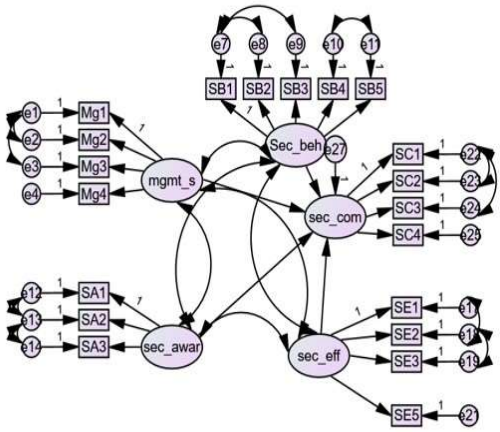

Figure 3: The refined measurement model

The study hypotheses are either accepted or rejected based on the Probability Value (P-value) and the Standardized Coefficient (β) measurements. For a hypothesis to be accepted, the probability value (P-value) must be less than 0.05. An independent variable's predictive power is measured by its standard coefficient. Figure 4 shows the standardized coefficients for each hypothesis concerning each other. It is evident from the table 7 that the probability value and R2 accepted the proposed hypotheses.

Table 7: Hypothesis Testing results

H#	Standardized Coefficients (β)	Probability Value (P-value ≤ 0.05)	Adjusted R^2	Results
H1	0.719	0.001	0.515	Accepted
H2	0.781	0.000	0.609	Accepted
H3	0.691	0.004	0.474	Accepted
H4	0.744	0.000	0.551	Accepted

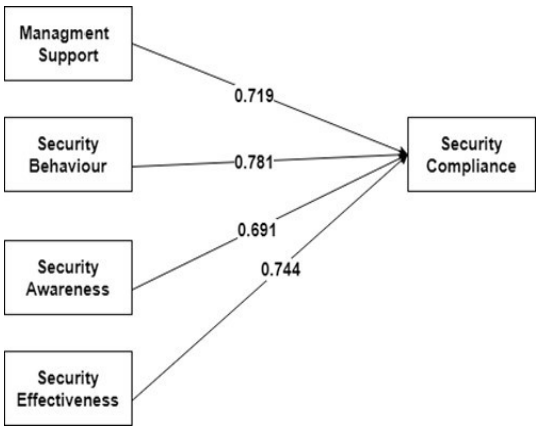

Figure 4: The outcome of hypotheses testing

6. RESULTS AND DISCUSSION

According to our findings, healthcare facilities and other Saudi Arabian organizations covered by the security agreement must fully comply. The study's main objective was to assess and empirically validate a theoretical model that uses management support, security awareness, security behavior, and security effectiveness to predict security behavior, energy, and thus security compliance in the healthcare center. A web-based survey was designed using previously validated scales to test the impact of these variables on care center security compliance. In this study, healthcare workers were the primary focus; a whopping 94.1% of the approximately 208 healthcare professionals were asked to participate in the survey. How do management support, security awareness, behavior, and effectiveness influence a healthcare center? This was the primary research issue addressed by this study. Security effectiveness has a favorable effect on security compliance, as the study's theoretical model indicated. Additional evidence shows that the dependent variables SC were significantly affected by the independent variables SA, SE, SB, and MG. As a result of this analysis, a new construct was identified: management support and its impact on security effectiveness and security behavior and hence security compliance in AMCs. The results and correlation analyses showed that management

support had a substantial weight in predicting security compliance related to security behavior.

6.1 Comparison Results

According to [38], [39], and [40], the author's findings empirically confirmed the research stated in the literature that management support is an essential factor that influences security compliance. A second issue is that the concept of security awareness has only been used sparingly in IT and security studies, but has yet to be implemented in an academic medical setting. Security awareness and its effect on security effectiveness and behavior and hence security compliance were discovered due to this inquiry. Correlation analysis revealed that security awareness was the most critical factor in determining whether or not a person would comply with security regulations. Researchers [41], and [42] found that security awareness is a key concept that influences security compliance, and the author's findings experimentally confirmed their findings.

The third issue is that security efficacy has been used sparingly in IT and information security research but not in academic medicine. A novel concept was discovered in this study: security effectiveness and its relationship to security conformance. Security effectiveness was a substantial predictor of security compliance in correlation analyses. According to the author's findings, management support is directly linked to security compliance, which supports previous studies by [43], and [44].

It should be noted that the security behavior construct has been used in the IT and information security research domains to a limited extent, but not in an academic medical environment. As a result, a new concept was discovered in this study: security behavior and the impact it has on security compliance. Security behavior was found to be a significant predictor of security compliance [41]. It shows that computer self-efficacy influences security compliance. But the authors' findings also show the need for more research into the elements related with secure behavior in computers [41].

6.2 Main Investigations

This investigation has substantial implications for future research. To predict security effectiveness and behavior, the author constructed a theoretical model employing the factors of management support, security awareness, security culture, and computer self-efficacy. Based on a thorough review of the scientific literature, the author chose the independent and dependent variables for the model. Consequently, the two main contributions of this investigation to the literature on technology acceptance and security effectiveness include: (a) the development and validation of a theoretical model for predicting security effectiveness and behavior, as well as the determination of the most significant factors that affect security effectiveness and behavior. These findings support healthcare center to realize the need to maintain strict security standards.

The findings of this study have three practical implications. In the first place, the findings of this study serve as a guide for healthcare workers and organizations participating in security compliance initiatives. For healthcare centers, the findings of this study contribute knowledge that may be used to improve information security and regulatory compliance. So this investigation can be used to (a) decrease data security breaches; (b) improve security measures required by the increased use of IT in healthcare; (c) better prepare for the stricter enforcement and increased federal audits of Security Rule compliance; (d) improve compliance with the new federal regulations that extend the Security Rule. For academics and practitioners in information security, the research model established as a result of this analysis can provide a framework for understanding the current security requirements applied by the healthcare institution. Healthcare organizations will be better equipped to understand and comply with the Security Rule due to our research and the accumulated knowledge.

6.3 Limitations

Currently, the investigation focuses on the impact of non-compliance with security standards on the healthcare facility. It's also possible that the data may have changed since it was gathered at a specific moment in time. No moderator factors on acceptance, such as age or experience, are examined in this study. It is also important to point out that this study's primary focus was on quantitative research, which may have limited its capacity to provide a comprehensive view at healthcare center and user perception. Because this study relied on a convenient sample for Saudi healthcare workers, the findings cannot be generalized to other locations. The study constraints also suggest new directions for inquiry.

Finally, the respondents were sent the Web-based survey instrument through email without any additional inducement to complete it. One explanation for the low response rate is that respondents were willing to self-select and spend the time required to complete the survey. There may have been an underrepresentation of IT professionals

who don't care about security compliance as a result of their self-selection.

7. CONCLUSION AND FUTURE WORK

In the end, some new areas of study were discovered. For the current study, there was no limit on the number of healthcare facilities respondents might visit. As a result, future studies might ensure that up to one person from each organization participates in the poll. The involvement of a member in an organization's security compliance program may affect their opinions of security compliance. As a result, there is more needs to do beneficial research on security compliance perceptions from a broader range of healthcare professionals (e.g., executive management, line management, financial, clinical, and technical) within the same healthcare center. In future studies, it may be necessary to ask respondents if they have sufficient awareness of their company's information security program. Participants in this study were presumed to have a working knowledge of their company's IT and information security program because they were all IT professionals. Health maintenance organizations, physician practice groups, hospital networks, independent practice associations, physician-sponsored networks, managed care organizations, clinics, and preferred providers might increase the generalizability of this study's findings.

Security framework, perceived security, perceived usefulness, resistance to change, and trust should all be examined in future research. These other factors were omitted from the study to keep the scope manageable. Many elements influence security compliance, and our investigation needed to be more comprehensive. Security compliance at healthcare centers was examined due to the study's independent variables, Mg, SE, SA, and SE. Actual security compliance, on the other hand, needed to be assessed. Investigations could determine how well the hospitals are doing in terms of securing themselves.

Medical professionals' non-compliance with corporate security policies while utilizing personal mobile devices at work was the focus of the study's contribution to the general business technology challenge. So that solutions could be devised to address and restrict non-compliance, the study analyzed the factors influencing medical professionals' non-compliance with organizational security policies. As a result, training programs can be designed to address the underlying causes of non-compliance. Participants agreed that they had enough training between the time they were hired and the time they were considered beginner doctors. Study findings show that computer-based training initiatives may not be as efficient in raising phishing awareness as annual face-to-face and frequent training exercises.

To conclude, the results of this study show that healthcare leadership, as represented in part by the participants, recognizes the importance of organizational backing for cybersecurity initiatives, as well as an understanding of the importance of security culture. No one reported that computer self-effectiveness had an impact on security compliance. Understanding management support, security awareness, security culture, and computer self-efficacy is essential to ensure compliance with the Security Rules. Knowledge gained from future research on factors influencing management support, security awareness, and security effectiveness in practice could lead to better security compliance.

For future investigations, studies are needed to identify the causes of non-compliance with security standards in healthcare facilities. A comparative analysis of security compliance reasons and barriers should also be conducted. Future research could use a mixed-method approach (quantitative and qualitative) to gain a complete understanding.

ACKNOWLEDGMENT

This work was supported by the Deanship of Scientific Research, Vice Presidency for Graduate Studies and Scientific Research, King Faisal University, Saudi Arabia [Grant No. GRANT2649].

REFERENCES:

[1] S. T. Alanazi, M. Anbar, S. Ebad, S. Karuppayah, and H. Al-Ani, “Theory-Based Model and Prediction Analysis of Information Security Compliance Behavior in the Saudi Healthcare Sector”, *Symmetry*, Vol. 12, No. 9, 2020, pp. 1544.

[2] N., Al-Kahtani, S., Alrawiai, M., Al-Zahrani, R., Abumadini, A., Aljaffary, B., Hariri, and A., Alumran, “Digital health transformation in Saudi Arabia: A cross-sectional analysis using Healthcare Information and Management Systems Society’digital health indicators”, *Digital Health*, Vol. 8, 2022, pp. 1-9.

[3] P., Dadhich, “Security of Healthcare Systems with Smart Health Records Using Cloud Technology”, *In Machine Learning with Health*

Care Perspective, Springer, Cham, 2020, pp. 183-198.

[4] MOH. Overview of E-Health - Overview of E-Health. https://www.moh.gov.sa/en/Ministry/nehs/Overview-of-eHealth/Pages/Overview-of-eHealth.aspx, (online; accessed 10/10/2021).

[5] E., Chanda, "Global Health Security: Crises Assessment", *Capacities, and Response Management. Handbook of Global Health*, 2020, pp. 1-20.

[6] A. Almazroi, F., Mohammed, H., Al-Kumaim, and M., Hoque, "An empirical study of factors influencing e-health services adoption among public in Saudi Arabia", *Health Informatics Journal*, Vol. 28, No. 2, 2022.

[7] H., Wahsheh, and M. Al-Zahrani, "Secure and usable QR codes for healthcare systems: the case of covid-19 pandemic", *In 2021 12th International Conference on Information and Communication Systems (ICICS)*, *IEEE*, May 2021, pp. 324-329.

[8] N., Guhr, B., Lebek, M., Breitner, "The impact of leadership on employees' intended information security behaviour: An examination of the full-range leadership theory", *Information Systems Journal*, Vol. 29, No. 2, 2019 pp. 340-362.

[9] A., AlKalbani, H., Deng, B., Kam, and X., Zhang, (2017). "Information Security Compliance in Organizations: An Institutional Perspective", *Data and Information Management*, Vol. 1, No. 2, 2017, pp. 104–114.

[10] K., Skouby, P., Dhotre, L., Williams, and K., Hiran, "5G, Cybersecurity and Privacy in Developing Countries", *CRC Press*, 2023.

[11] S., Acharya, and N., Werts, "Toward the Design of an Engagement Tool for Effective Electronic Health Record Adoption", *Perspectives in Health Information Management*, Vol. 16, 2019, pp. 1-15.

[12] O., McDermott, I., Foley, J., Antony, M., Sony, M., Butler, "The Impact of Industry 4.0 on the Medical Device Regulatory Product Life Cycle Compliance", *Sustainability*, Vol. 14, No. 21, 2022, pp. 14650.

[13] A., Althumairi, A., Alzahrani, T., Alanzi, S., Al Wahabi, S., Alrowaie, A., Aljaffary, and D., Aljabri, "Factors affecting compliance with national accreditation essential safety standards in the Kingdom of Saudi Arabia", *Scientific Reports*, Vol. 12, No. 1, 2022, pp. 1-9.

[14] Y., Li, and A., Albarrak, "An informatics-driven intelligent system to improve healthcare accessibility for vulnerable populations", *Journal of Biomedical Informatics*, Vol. 134, 2022, pp. 104196.

[15] S., Hamid, M., Roslan, A., Norman, N., Ghani, and Z., Jaafar, "Existing Framework and the Use of Emerging Technology in Healthcare and Healthy Lifestyle: A Review", *In 2021 International Conference on Computer Science and Engineering (IC2SE)*, IEEE, Vol. 1, 2021 pp. 1-9.

[16] F., Alanezi, "Factors affecting the adoption of e-health system in the Kingdom of Saudi Arabia", *International Health*, Vol. 13, No. 5, 2021, pp. 456-470.

[17] M., Al-Bohnayyah M., and H., Wahsheh, "Towards Developing Medical Sentiment Analysis Model", *NeuroQuantology*, Vol. 20, No. 17, 2022, pp. 238-244.

[18] A., Alshahrani, H., Williams, and K., MacLure, "Investigating Health Managers' Perspectives of Factors Influencing Their Acceptance of eHealth Services in the Kingdom of Saudi Arabia: A Quantitative Study", *Saudi Journal of Health Systems Research*, Vol. 2, No. 3, 2022, pp. 114-127.

[19] J., Yuanxiang and H., Elizabeth Hoffman, "*Information Security Policy Compliance*", (online; accessed 10/10/2021). https://lib.dr.iastate.edu/cgi/viewcontent.cgi?article=1094&context=econ_workingpapers

[20] N. Humaidi, and V., Balakrishnan, "Indirect effect of management support on users' compliance behaviour towards information security policies", *Health Information Management Journal*, Vol. 47, No. 1, 2018, pp. 17-27.

[21] K., Alsulame, M., Khalifa, and M., Househ, "eHealth in Saudi Arabia: Current Trends Challenges and Recommendations", *ICIMTH*, Vol. 213, 2015, pp. 233-236.

[22] A., Najjar, B., Amro, and M., Macedo, "The adoption level of electronic medical records in hebron hospitals based on the electronic medical record adoption model (EMRAM)", *Health Policy and Technology*, Vol. 10, No. 4, 2021, pp. 100578.

[23] J. Sorace, H., Wong, T., DeLeire, D., Xu, S., Handler, B., Garcia, and T., MaCurdy, "Quantifying the competitiveness of the electronic health record market and its implications for interoperability", *International Journal of Medical Informatics*, Vol. 136, 2020, pp. 104037.

[24] I., Hwang, R., Wakefield, S., Kim, and T., Kim, "Security awareness: The first step in information security compliance behavior". *Journal of Computer Information Systems*, Vol. 61, No. 4, 2021, pp. 345-356.

[25] T., Ryutov, N., Sintov, M., Zhao, and R., John, "Predicting information security policy compliance intentions and behavior for six employee-based risks", *Journal of Information Privacy and Security*, Vol. 13, No. 4, 2017, pp. 260-281.

[26] M., Furukawa, N., Eldridge Y., Wang and M., Metersky, "Electronic Health Record Adoption and Rates of In-hospital", *Journal of Patient Safety*, Vol. 16, No. 2, 2017, pp. 137–142.

[27] A., Hossain, R., Quaresma, and H., Rahman, "Investigating factors influencing the physicians' adoption of electronic health record (EHR) in healthcare system of Bangladesh: An empirical study", *International Journal of Information Management*, Vol. *44*, 2019, pp. 76–87.

[28] M., Sayed, "Knowledge, attitude and behaviour of dental health care providers towards health Electronic record systems in Saudi Arabia", *Health Information & Libraries Journal*, Vol. 38, No. 3, 2021, pp. 194-202.

[29] A., Holmgren, N., Downing, W., Bates, D., Shanafelt, A., Milstein, D., Sharp, C. D., Cutler, S., Huckman, and A., Schulman, "Assessment of Electronic Health Record Use Between US and Non-US Health Systems", *JAMA Internal Medicine*, Vol. 181, No. 2, 2021, pp. 251–259.

[30] P., Mulgund, P., Mulgund, R., Sharman, and R., Singh, "The implications of the California Consumer Privacy Act (CCPA) on healthcare organizations: Lessons learned from early compliance experiences", *Health Policy and Technology*, *10*(3), 2021, pp.100543.

[31] W., Pierre-Francois, and I., Guzman, "Factors that influence HIPAA Secure compliance in small and medium-size healthcare facilities", *KSU Proceedings on Cybersecurity Education, Research and Practice*, 2020, pp. 1-23.

[32] T., Rosenbloom, L., Smith, J., Bowen, J., Burns, L., Riplinger, and H., Payne, "Updating HIPAA for the electronic medical record era", *Journal of the American Medical Informatics Association*, Vol. 26, No. 10 , 2019, pp. 1115–1119.

[33] S., Altamimi, "Investigating and mitigating the role of neutralisation techniques on information security policies violation in healthcare organisations", *Doctoral dissertation, University of Glasgow*, 2022, pp. 1-294.

[34] Ali, Z., and B. Bhaskar, "Basic statistical tools in research and data analysis", *Indian Journal of Anaesthesia*, Vol. 60, No. 9, 2016, pp. 662.

[35] F., Hair, J., Risher, M., Sarstedt, M., Ringle, "When to use and how to report the results of PLS-SEM", *European business review*, Vol. 31, No. 1, 2019, pp. 2-24.

[36] A., Maydeu-Olivares, "Goodness of fit assessment of item response theory models", *Measurement: Interdisciplinary Research and Perspectives*, Vol. 11, No. 3, 2013, pp. 71-101.

[37] J. Hair, G., Hult, M., Ringle, C. M., Sarstedt, N., Danks, and S., Ray, "Evaluation of reflective measurement models", *In Partial Least Squares Structural Equation Modeling (PLS-SEM) Using R, Springer, Cham,* 2021, pp. 75-90.

[38] G., Barry, and J., Grossmeier, "Is your incentive strategy sound? Guidelines for designing a HIPAA compliant wellness program", *Employee Benefit Plan Review*, Vol. 64, No. 1, 2009, pp. 5-8.

[39] P., Logan, and D., Noles, "Protecting patient information in outsourced telehealth services: Bolting on security when it cannot be baked in", *International Journal of Information Security and Privacy (IJISP)*, Vol. 2, No. 3, 2008, pp. 55-70.

[40] J., Loghry, and C., Veach, "Enterprise Risk Assessments Holistic Approach Provides Companywide Perspective", *Professional safety*, Vol. 54, No. 02, 2009.

[41] D., Lending, and T., Dillon, "The effects of confidentiality on nursing self-efficacy with information systems", *International Journal of Healthcare Information Systems and Informatics (IJHISI)*, Vol. 2, No. 3, 2007, pp. 49-64.

[42] B., Medlin and J., Cazier, "An empirical investigation: Health care employee passwords and their crack times in relationship to hipaa security standards", *International Journal of Healthcare Information Systems and Informatics (IJHISI)*, Vol. 2, No. 3, 2007, pp. 39-48.

[43] S., Lineberry, "The human element: The weakest link in information security", *Journal of Accountancy*, Vol. 204, No. 5, 2007, pp. 44.

[44] M., Sveen, T., Jeppesen, S., Hauerslev, T., Krag, and J., Vissing, "Endurance training: an effective and safe treatment for patients with LGMD2I", *Neurology*, Vol. 68, No, 1, 2007, pp. 59-61.