Factors Influencing Information Security Policy Compliance Behavior "A Case – Study Healthcare Workers in a Private Hospital in Mogadishu – Somalia"

Zakarie Abukar Aweis
Computer Science & IT
Asia e University
Selangor, Malaysia

Mohamed Adam Isak Abdirahman
Computing Sciences
Darul Hikmah University (DHU)
Mogadishu, Somalia

Abdulkadir Jeilani Mohamud
Computer Science & IT
Mogadishu University
Mogadishu, Somalia

Abstract:- Information security policy compliance is crucial for safeguarding sensitive data in healthcare settings. This study investigates the factors influencing information security policy compliance behavior among healthcare workers at a private hospital in Mogadishu, Somalia. Findings reveal that beliefs in the importance of information security, effectiveness of communication and training programs, usability of security tools, and socio-cultural factors significantly impact compliance behavior. The study provides insights for healthcare administrators and policymakers to enhance compliance strategies in healthcare organizations.

Keywords:- *Information Security Policy Compliance; Healthcare Workers; Private Hospital.*

I. INTRODUCTION

Information security in healthcare settings is vital to protect patient data against breaches and unauthorized access (Adan Damey & Dhaka, 2019). Despite stringent policies, compliance among healthcare workers remains a challenge globally, including in Somalia (Hashi & Isa, 2015). Understanding the factors influencing compliance behavior is crucial for designing effective strategies to mitigate risks and enhance security practices in healthcare organizations.

A. The Healthcare Industry in Somalia

The healthcare industry in Somalia has faced numerous challenges over the years due to ongoing political instability, armed conflicts, and limited infrastructure. Despite these difficulties, healthcare providers in the country strive to deliver essential medical services to the population.

The sector comprises both public and private healthcare institutions, with private hospitals playing an increasingly significant role in catering to the healthcare needs of the population, especially in urban centers like Mogadishu. (Hashi & Isa, 2015)

The healthcare system in Somalia is decentralized, with healthcare services delivered at the regional and district levels. The lack of a centralized healthcare structure poses unique challenges in coordinating efforts, sharing information, and ensuring consistent standards of care across the country. Furthermore, the healthcare system's limited resources and capacities have led to disparities in healthcare accessibility and quality between urban and rural areas. (Hashi & Isa, 2015)

Reliable data collection and access across a range of sectors, including healthcare, education, and economics, present major issues for Somalia. One major problem impeding efficient policymaking, resource allocation, and development planning is the lack of data. This section examines the causes of Somalia's data scarcity, the effects of that scarcity, and possible ways to enhance data access and gathering.

This is mainly the case for quantitative and qualitative socio-economic data or information. Where facts are available, certain are often incomplete. In addition to the typical absence regarding information, such as is available is often outdated. This is principally due to the fact the situation of Somalia adjustments often and substantially. Difficulties often arise when gathering current data because the statistics is currently not accessible. In emergency situation, information structures then statistics series is devoted low priority among most of Somalia (Warsame et al., 2015)

B. Information Security Policies in Healthcare Organizations

In response to the growing cybersecurity risks, healthcare organizations in Somalia, including private hospitals, have recognized the importance of robust information security policies. These policies are designed to safeguard patient data, ensure the confidentiality and integrity of medical records, and foster a culture of security awareness among employees.

Data encryption, access controls, password policies, employee training, and incident response procedures are just a few examples of the various security measures covered by information security policies. The protection of sensitive healthcare data and the reduction of cybersecurity risks depend heavily on compliance with these standards.

Information security is required to protect organization data from information security threat such as virus and unauthorized users. Information security threats can be categorized into two categories: internal threat and external threat. External threat is caused by outsiders and it is not a major issue in information security because many organizations have implemented advanced security technologies such as smart card and biometrics. Until recently, the main critical information security issue identified is internal threat, where is caused by internal factors, mainly the employees‟ poor users‟ behavior such as Many studies have found that the employees of an organization could be the real culprit of most security breaches whether it was done intentionally or unintentionally (Humaidi & Balakrishnan, 2015a).

II. LITERATURE REVIEW

According to (Ranta, 2010) Health information systems (HIS) has been introduced in Malaysia in the late 90s. Since then, different government and private hospitals have been utilizing HIS for various purposes. HIS is a multipurpose system that holds records of patients, hospital management, and staff. HIS can be used as a web application or accessed from the internet for data updates and storage. Besides, ease of system accessibility can be vulnerable. The data of HIS is susceptible, and it requires more security and protection. Appropriate security is needed for the personal health information of patients. Regardless of the nature of the information in healthcare environments, users do not take infosec seriously. Some employees have legitimate access to HIS, and negligence can harm the confidentiality of patients' personals records.

According to (Ranta, 2010) The advancement of information communication technology in healthcare institutions has increased information security breaches. Scholars and industry practitioners have reported that most security breaches are due to negligence towards organizational information security policy compliance (ISPC) by healthcare employees such as nurses. There is, however, a lack of understanding of the factors that ensure ISPC among nurses, especially in developing countries such as Malaysia.

Information security is crucial for maintaining the privacy, availability, and integrity of data. Compliance with information security policies is crucial for ensuring that information security controls are applied and adhered to. Given that they handle and keep a lot of sensitive patient data, healthcare institutions are particularly susceptible to cyberattacks. Due to their responsibility for establishing and adhering to the organization's information security policy, healthcare professionals are essential to information security compliance.

Several earlier research looked into how healthcare professionals and personnel from other industries complied with information security policies. These studies have revealed a wide range of elements, such as individual knowledge, organizational support, training programs, and technological usability that have an impact on compliance behavior. However, it is crucial to understand that the healthcare context provides specific difficulties and factors that might have a different impact on compliance behavior.

An in-depth insight of the variables impacting the conduct of healthcare professionals in a private hospital in Mogadishu, Somalia, is provided by this review of the literature in Africa. This study prepares the stage for the empirical investigation by looking at human, organizational, and technology elements as well as theoretical models of compliance behavior. The results of this study will help healthcare institutions in Somalia and possibly other situations like it improve their information security procedures and foster a compliance culture. (Ranta, 2010)

A. Information Security in Healthcare

Due to the private and sensitive nature of patient information, information security in healthcare is of the utmost importance. The management of patient records, diagnostic information, and medical histories has become more and more dependent on information technology in the healthcare industry. But this digitalization has also made healthcare institutions more vulnerable to different security risks. Patient data breaches endanger individual privacy, cause financial losses, and harm the standing of healthcare providers.

Although there is a clear need for strong information security policies and procedures, the success of these measures strongly depends on the compliance behavior of healthcare professionals. The term "compliance behavior" describes how people behave when they follow the rules and guidelines that have been established by their organizations to protect the privacy, availability, and integrity of information. In order to create efficient information security rules, it is essential to comprehend the variables that affect compliance behavior.

According to (Narayana Samy et al., 2010) The international standard for health informatics, Information Security Management in Health using ISO/IEC 27002 (ISO27799:2008), defines HIS as a 'repository of information regarding the health of a subject of care in computerprocessable form, stored and transmitted securely and accessible by multiple authorized users.

Different standards and writers have developed different kinds of threat categories. This ISO standard, for instance, divided threats to HIS into 25 categories. Internal and external risks are the two main categories into which threats to hospital information systems have been divided. Employee actions including indifference, curiosity, recklessness, inadequate behavior, stealing someone else's login, and sharing their password with another employee are all examples of internal threats. Attacks from viruses and malware, hackers, and trespassers are examples of external threats.

➢ *Security Threats In Information Systems*

Threat is defined as any unexpected or potential cause of an unwanted incident that impact negatively on a system or organization. Basically, there are three major categories of threat source

- Natural threats: events resulting from forces of nature such as floods, earthquakes, tornadoes, landslides, and electrical storms.
- Human threats: events that are either enabled by or caused by human beings, including unintentional acts (inadvertent information entry) and deliberate acts (network-based attacks, malicious software, unauthorized access to confidential information).
- Environmental threats: incidents or conditions such as pollution, chemical spills, and liquid leakage.

According to (Narayana Samy et al., 2010) To discuss information security challenges, a structured classification of threats is necessary. Threats to information systems have been categorized in numerous ways. Threats can be categorized based on their actions and effects. The following categories of actions are possible: observe, eliminate, alter, and imitate threats. Threats to integrity, execution, misrepresentation, and repudiation are a few examples of consequences. Security risks can also be divided into interruption, interception, modification, and fabrication categories. Threats can also be divided into groups based on the kind of assets at risk.

There are two perspectives through which threats in information systems might be viewed. Based on danger agents, the first one. Authorized users, unauthorized users, and environmental factors are different categories of threat agents. The second one uses penetration-style methods. Physical, personnel-related, hardware, software, and procedural intrusion techniques are all possible. Another study highlighted other threat categories, including intentional software attacks, human failure or error, technical device failures or errors, natural disasters, and technological obsolescence (Narayana Samy et al., 2010).

B. Factors Influencing Information Security Policy Compliance Behavior

According to (Humaidi & Balakrishnan, 2015b) If employees' conduct toward information security can be controlled and managed appropriately, ISPs can be implemented more successfully. This can present security risks to the organization if it cannot be appropriately controlled or monitored. Promoting appropriate information security behavior and preventing inappropriate information behavior among company employees will increase the effectiveness of information systems security.

According to the study, security incidents can be reduced and the effectiveness of information system security can be boosted if employee compliance behavior with information security policies is acceptable. The idea that security compliance behavior can encourage security assurance behavior is backed by additional publications. Security assurance behavior is described as behavior that actively works to safeguard organization IS, such as taking security precautions and reporting any security incidents that may occur in the organization. Security compliance behavior is defined as behavior that does not violate organization ISPs (Humaidi & Balakrishnan, 2015b).

There are several reasons why users did not comply on security rules and procedures which are they feel the security rules and policy is too strict, lower usability, nuisance, complicated and difficult to follow.

Table 1. Summary of the Factors Influencing Information Security Policy Compliance Behavior "A case – study healthcare workers in a private hospital in Mogadishu – Somalia"

Category	Factors	Description
Individual Factors	Perceived Importance of Information Security	Belief in the significance of information security.
	Confidence in Following Security Protocols	Self-assurance in adhering to security guidelines.
	Awareness of Security Risks	Knowledge of potential security risks and threats.
Organizational Factors	Clarity of Policy Communication	Clear and effective communication of security policies.
	Effectiveness of Training Programs	Comprehensive training on information security.
	Organizational Commitment to Security	Strong commitment from hospital leadership to security.
Technological Factors	Usability of Security Tools and Systems	User-friendliness of information security tools.
	Reliability of Hardware and Software	Dependability of technology used for security.
	Presence of Technological Barriers	Technological obstacles that hinder compliance.
	Organizational Culture	Culture within the hospital that prioritizes security.

Cultural and Socio-Economic Factors	Socio-Economic Factors	Socio-economic status influencing compliance.

C. *Theoretical Models of Compliance Behavior*

In the area of information security, a number of theoretical models have been put out to explain compliance behavior. Both the Theory of Planned Behavior (TPB) and the Protection Motivation Theory (PMT) have already been mentioned. The Extended Parallel Process Model (EPPM) and the Health Belief Model (HBM) have both been used to analyze information security compliance in healthcare settings. These models offer important new perspectives on the motivational and cognitive facets of compliance behavior (Kim & Kim, 2017).

There are many theoretical models of compliance behavior in healthcare workers. According to (Kim & Kim, 2017) One of the most prominent models is the Health Compliance Model-II (HCM-II) which is posited to address the multivariate, dynamic, and idiosyncratic nature of predicting adherence to health behaviors.

D. *Theoretical Framework*

The theoretical framework guiding this study draws from several established theories and models:

➢ *Theory of Planned Behavior*

(Bosnjak et al., 2020): This theory posits that an individual's intention to perform a behavior is influenced by their attitude toward the behavior, subjective norm, and perceived behavioral control. In the context of this study, it informs the exploration of individual factors influencing compliance behavior.

➢ *Organizational Culture and Commitment Theory*

(Hartnell et al., 2011)**:** This theory highlights the significance of organizational culture and commitment in shaping employee behavior. It informs the examination of organizational factors affecting compliance.

➢ *Technology Acceptance Model*

(Wiederhold & Reality, 2015): This model explores factors that influence the adoption and use of technology. It informs the investigation of technological factors impacting compliance.

E. *Conceptual Framework*

The conceptual framework synthesizes the theoretical perspectives into a cohesive model specific to this study:

➢ *Individual Factors*

Drawing from the Theory of Planned Behavior, this component includes variables such as perceived importance of information security, confidence in following security protocols, and awareness of security risks.

➢ *Organizational Factors*

Rooted in Organizational Culture and Commitment Theory, this component encompasses variables like the clarity of policy communication, the effectiveness of training programs, and the hospital's commitment to information security.

➢ *Technological Factors*

Informed by the Technology Acceptance Model, this component includes variables related to the usability and accessibility of information security tools and systems.

F. *Hypothesis*

Numerous predictable factors that might either help or impede information security adoption and use in private health care have an impact on it. The study questions that serve as the foundation for the hypothesis suggest that the requirement for specific skills and knowledge may be a major influence on how medical staff in private hospitals in Mogadishu, Somalia, behave with regard to adhering to information security policies.

This study looks at the opportunities and difficulties associated with the application of information security in Mogadishu's healthcare system. An introduction to the history of computer use in healthcare is followed by a discussion of the results of recent international research on the variables influencing information security policy compliance behavior in healthcare, and a comparison of those findings to those found in health care facilities in Mogadishu. The acceptance and use of modern information and communication technologies in the field of healthcare is discussed in this study, along with advice for organizational, corporate, public, and governmental leadership.

Here are some hypotheses:

- Hypothesis H1: Healthcare workers belief in the importance of information security is positively related to their compliance with information security policies at the private hospital in Mogadishu, Somalia.
- Hypothesis H2: The effectiveness of communication and training regarding information security policies within the hospital is positively related to healthcare workers' compliance with those policies.
- Hypothesis H3: The usability and accessibility of information security tools and systems in the hospital positively influence healthcare workers compliance with information security policies.
- Hypothesis H4: Socio-cultural and economic factors, such as the hospital's organizational culture and socio-economic status of healthcare workers, positively influence their compliance with information security policies.

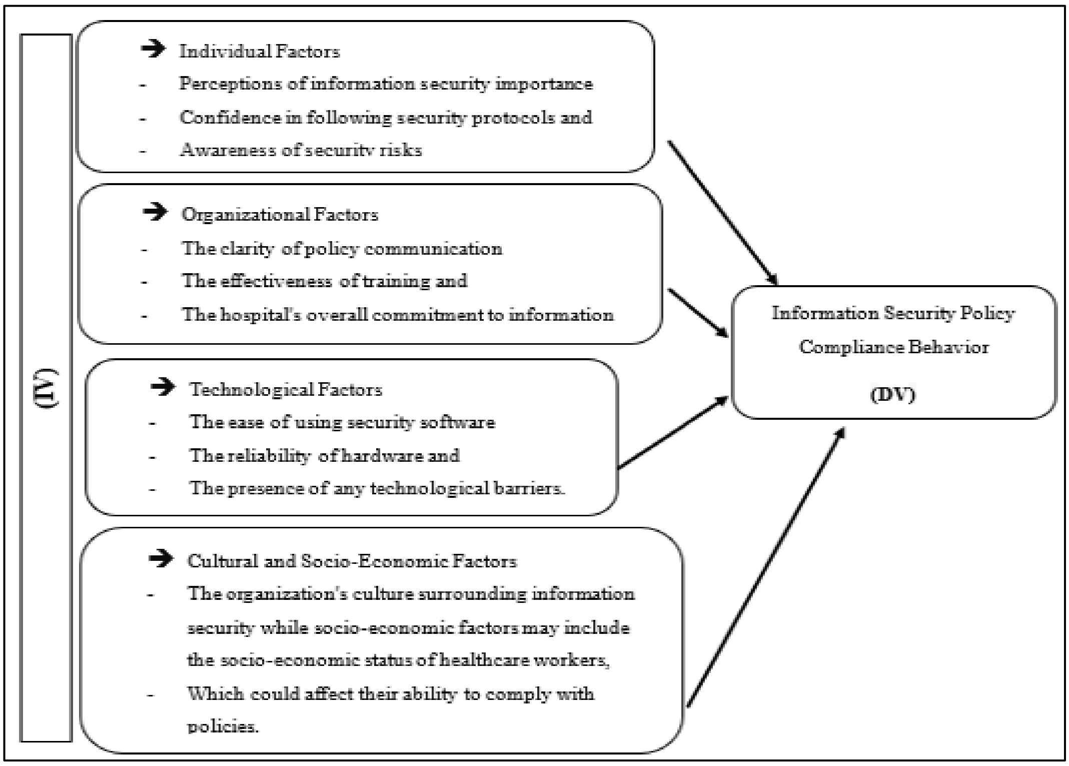
(IV)
➔ Individual Factors
- Perceptions of information security importance
- Confidence in following security protocols and
- Awareness of security risks
➔ Organizational Factors
- The clarity of policy communication
- The effectiveness of training and
- The hospital's overall commitment to information
➔ Technological Factors
- The ease of using security software
- The reliability of hardware and
- The presence of any technological barriers.
➔ Cultural and Socio-Economic Factors
- The organization's culture surrounding information security while socio-economic factors may include the socio-economic status of healthcare workers,
- Which could affect their ability to comply with policies.
Information Security Policy Compliance Behavior
(DV)

Fig.1: Theoretical framework

III. METHODOLOGY

➢ *Theoretical Framework*

The theoretical framework guiding this study draws from several established theories and models:

- Theory of Planned Behavior (Bosnjak et al., 2020): This theory posits that an individual's intention to perform a behavior is influenced by their attitude toward the behavior, subjective norm, and perceived behavioral control. In the context of this study, it informs the exploration of individual factors influencing compliance behavior.
- Organizational Culture and Commitment Theory (Hartnell et al., 2011): This theory highlights the significance of organizational culture and commitment in shaping employee behavior. It informs the examination of organizational factors affecting compliance.
- Technology Acceptance Model (Wiederhold & Reality, 2015): This model explores factors that influence the adoption and use of technology. It informs the investigation of technological factors impacting compliance.

➢ *Research Design*

Research design is the blue print for gratifying goals and answering questions (Cooper, D. R., Schindler, P. S., & Sun, 2006). The study will use descriptive research design to explain the factors influencing information security policy compliance behavior Healthcare workers in a private hospital in Mogadishu Hospitals.

According to (Approach, 2016) observed that descriptive survey research is intended to offer statistical data regarding educational issues that attract educators and policy makers. It is a method of acquiring data that involves asking a sample of people a questionnaire.

According to (Hodgkinson & Clarke, 2007), Descriptive studies are frequently created to gather data on characteristics of people, events, and situations. Quantitative and qualitative data may remain in a descriptive study design. The quantitative research design was chosen because it helps the government produce true and trustworthy results data and is most pertinent to studying information security in health care, in this example in the city of Mogadishu.

A survey with standardized questions will be undertaken among the staff of the hospitals in Mogadishu. Health care employees are the dependent variable and factors impacting information security policy compliance behavior are the independent variables in the study. Three variables—factors affecting, information security policy compliance behavior, and healthcare workers—serve as the study's compass. Information security policy compliance behavior in the healthcare workforce, Mogadishu Hospitals, is influenced by individual factors, organizational factors, technological factors, cultural factors, and socio-economic factors. These four areas will be taken into consideration in the variable of factors influencing.

The questionnaire's flaws and any unclear or ambiguous items will be found using the results of the pilot study. Before the researcher begins collecting data, feedback from the pilot study will be used to correct any flaws in the questionnaire.

- *Sampling*

The study is planned to adopt a quantitative research design. The population under the study protected specific 200 individuals selected from the population, these people who are entrusted with top administrators, physician, nurses, patients and other department’s staff in Mogadishu Private Hospitals. The sampling unit in this study is going to stay the randomly selected hospitals in Mogadishu, from each hospital, fifteen (15) hospital administrators along with the top manager interviewed using questionnaires, will keep choice to be interviewed using random sampling technique. Based on Slovene’s formula, 129 samples randomly respondents had been selected from the target population. This was representative of the selected department from the total population in these Private Hospitals. The data collection instruments will be questionnaires for the administrator and staff of these hospitals.

n = N / (1 + N e2) = 200 / (1+200*0.052^2) =129

- *Data Collection Methods*

A structured questionnaire will be used to collect primary data. A structured questionnaire is a set of coded questions with well-defined patterns following a sequence regarding questions (Yusoff et al., 2021).

These are preferred so it are easy in imitation of take the chair yet bear temperate dependencies in the course of data analysis. A Likert range of one to five will be used after measure the extent to who the respondents agree and disagree with the questions.

Some questions will have a choice about other where respondents can mark other responses not included in the structured section. It will be divided in 2 parts.

Part I will comprise on demographic information about the respondent, theirs departments concerning work and their tenure including the Private hospital and general asking on Healthcare Workers basics.

Part II will take into account the overall aspects of the study, including the financial aspects. Healthcare Workers in Mogadishu Private Hospitals, how the Factor influences adoption of Information Security Policy Compliance Behavior in Mogadishu Hospitals, user perception in the adoption of Information Security of Mogadishu Private Hospitals, and whether skills and knowledge gaps are present at the conclusion. Factors affecting healthcare employees' compliance with information security policies in private hospitals in Mogadishu, Somalia.

- *Data Analysis Technique*

Quantitative data from the survey will be analyzed using statistical software, including descriptive statistics, regression analysis, and correlation analysis. The quantitative method of analysis will continue to be applied. Software called Statistical Packages for Social Sciences (SPSS) will have the variables coded and entered. Data will be gathered, coded, checked for mistakes, and then analyzed. In order to examine the data obtained from the research instruments, descriptive data, such as frequency distribution tables, percentages, means, and correlation coefficients, are typically used. Both the descriptive and numerical methodologies will be used in the study to summarize the data.

For simpler understanding, the presentation of the data will continue to use pie charts and graphs. This will enable a greater comprehension of the findings and results.

IV. RESULTS AND ANALYSIS

An examination of the information gathered from medi cal staff members in a private hospital in Mogadishu, Somal ia, provided important new information about the variables a ffecting adherence to information security policies.

The following is a summary of the findings:

- *Individual Factors*

Table 2. Individual Factors

Descriptive Statistics			
	N	**Mean**	**Std. Deviation**
The importance you place on information security in your daily work. Important	142	2.75	1.144
Please indicate your level of confidence in your ability to follow the information security policies and practices at our hospital.	142	3.11	1.428
How aware are you of the security risks associated with not complying with information security policies?	142	2.93	1.486
Valid N (listwise)	142		

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24JUL1238

➢ *Organizational Factors*

A perceptive investigation of respondents' opinions reg arding organizational commitment, communication, and trai ning with reference to information security in the healthcare sector.Three important aspects of the information security c ulture among 142 healthcare professionals are covered by ou r Study:

- Perception of Information Security Importance: Healthcare workers are more likely to follow security policies and procedures if they believe that information security is an essential part of their job. Their daily actions are influenced by this perception, which makes them follow defined procedures and take the appropriate safety measures to safeguard patient data.
- Training and Knowledge Updates: Consistent and thorough training initiatives have a big influence on participants' compliance behavior. According to our research, healthcare personnel are better able to apply information security policies when they receive regular training and updates. By keeping them updated on best practices and the newest risks, continuous education promotes a proactive security culture.
- Support and Guidance: A key component of compliance is having access to supervisors and information security specialists. Healthcare professionals are more likely to adhere to the right protocols if they have the option to seek advice when unsure about security precautions. By giving workers a safety net and reinforcing the value of compliance, this support system improves the organization's overall security culture.

Table 3. Organizational Factors

Descriptive Statistics			
	N	**Mean**	**Std. Deviation**
Rate the clarity of communication regarding information security policies within the hospital.	142	2.92	1.376
Have you received comprehensive training on information security policies and procedures?	142	2.99	1.324
To what extent do you believe the hospital management is committed to information security?	142	2.86	1.340
Valid N (listwise)	142		

➢ *Technological Factors*

An in-depth analysis of the user experience with information security tools and systems, as well as the technological challenges encountered by healthcare professionals in complying with information security policies. In this examination, we explore the perspectives and experiences of our 142 respondents within the healthcare sector.

Table 4. Technological Factor

Descriptive Statistics			
	N	**Mean**	**Std. Deviation**
How user-friendly do you find the information security tools and systems provided by the hospital?	142	3.40	1.363
Have you encountered any technological barriers that hinder your compliance with information security policies?	142	2.80	1.239
Valid N (listwise)	142		

➢ *Cultural and Socio-Economic Factors*

A comprehensive exploration of the factors influencing information security practices among our 142 healthcare professionals. In this analysis, we delve into two critical dimensions: the organizational culture of the hospital and the perceived impact of socio-economic factors on information security compliance.

Table 5. Cultural and Socio-Economic Factors

Descriptive Statistics			
	N	**Mean**	**Std. Deviation**
To what extent does the hospital's culture prioritize information security?	142	3.07	1.140
Do you believe your socio-economic status, such as income and education, affects your ability to comply with information security policies?	142	3.04	1.263
Valid N (listwise)	142		

- *Compliance Behavior*

Table 6. Compliance behavior

Descriptive Statistics			
	N	**Mean**	**Std. Deviation**
How frequently do you adhere to the information security policies and practices at the hospital?	142	2.93	1.096
Is there any reasons or challenges you face when complying with information security policies:	142	1.16	.370
I believe that complying with information security policies is essential to maintaining the confidentiality and integrity of patient information.	142	2.77	1.308
I regularly update my knowledge and skills related to information security to ensure compliance.	142	3.39	1.315
I consistently follow information security policies and procedures in my daily work.	142	2.92	1.343
I seek guidance and support from information security professionals or supervisors when uncertain about compliance with policies.	142	3.12	1.407
Valid N (listwise)	142		

- *Linear Regression Analysis*

A simple linear regression analysis was conducted based on 142 completed responses of the questionnaire collected from the healthcare workers operating in Mogadishu the capital city of Somalia. The linear relationship between the individual factor, organizational factor, technological factor , Cultural and Socio-Economic Factors as an independent variable with the information security compliance behavior as dependent variable. The linear regression will clarify whether the factor has significant effect on information security compliance behavior and healthcare workers according to the collected data through the questionnaire.

In this table shows:

- If P (significant) is less than your chosen significance level (e.g., 0.05), you can consider the hypothesis for that variable as accepted (statistically significant).
- If P (significant) is greater than or equal to your chosen significance level, you can consider the hypothesis for that variable as rejected (not statistically significant).

Based on the table:

- *Accepted Hypotheses:*

The hypothesis related to "Organizational Factors" is accepted because it has a significant

P-value (0.029) while the R^2 = 0.058.

The hypothesis related to "Cultural and socioeconomic Factors" is accepted because it has a significant p-value (0.020) while the R^2 = 0.049.

The constant term (intercept) is accepted as it is statistically significant (p-value: 0.000).

Table 7: Accepted Hypothesis

Variable	**Beta**	**T**	**P (significant)**	**R Square**
Constant	1.803	7.470	0.000	
Organizational Factors	0.123	2.200	0.029	0.058
Cultural and Socioeconomic Factors	0.117	2.345	0.020	0.049
a. Dependent Variable: Compliance behavior				

- *Rejected Hypotheses:*

The hypothesis related to "Individual Factors" is rejected because its p-value (0.069) is greater than the chosen significance level (e.g., 0.05) R^2 = 0.050.

The hypothesis related to "Technological Factors" is rejected because its p-value (0.627) and R^2 = 0.004 is much greater than the chosen significance level.

Table 8. Rejected Hypothesis

Variable	Beta	T	P (significant)	R Square
Constant	1.803	7.470	0.000	
Individual Factors	0.092	1.832	0.069	0.050
Technological Factors	-0.023	-0.486	0.627	0.004
a. Dependent Variable: Compliance behavior				

V. DISCUSSIONS AND IMPLICATIONS

In this section, we engage in a comprehensive discussion of the research findings, examining the relationships between the independent and dependent variables. We contextualize the results within the theoretical framework, offering insights into the significance of our observations.

The findings of our study provide valuable insights into the intricate dynamics surrounding information security policy compliance behavior among healthcare workers in a private hospital in Mogadishu, Somalia. Notably, our research confirms the significance of individual beliefs in the importance of information security in influencing compliance behavior. Healthcare workers who perceive information security as vital are more likely to adhere to established policies. Furthermore, the positive correlation between the effectiveness of communication and training programs and compliance underscores the need for targeted and comprehensive training initiatives. This suggests that healthcare institutions should invest in training programs that not only convey the importance of security but also equip employees with the knowledge and skills to implement security protocols effectively. These findings collectively contribute to a deeper understanding of the factors that drive compliance behavior in healthcare settings, offering practical insights for organizations striving to enhance their information security practices.

VI. LIMITATIONS OF THE STUDY

This subsection critically evaluates the limitations encountered during the research process. We assess methodological constraints, contextual factors, and data limitations, acknowledging their potential impact on the generalizability and scope of our findings.

It is imperative to acknowledge these limitations as they not only offer a more nuanced understanding of our research but also guide future research directions. By critically evaluating methodological, contextual, and data-related constraints, we provide researchers in this field with valuable insights into the complexities and challenges associated with studying information security policy compliance behavior among healthcare workers. While these limitations may impose constraints on the study's external validity, they also serve as a catalyst for further investigations aimed at uncovering the intricacies of compliance behavior within varying healthcare contexts. In essence, the limitations identified in this study pave the way for future research endeavors, emphasizing the dynamic and evolving nature of the field of information security policy compliance in healthcare settings.

VII. CONCLUSIONS AND RECOMMENDATIONS

A. Conclusions

Our study's conclusions have broader implications for the healthcare industry, offering actionable insights to healthcare administrators, policymakers, and organizational leaders. It is clear that promoting information security policy compliance requires a multifaceted strategy that addresses both individual beliefs and organizational culture. By investing in effective training programs, optimizing the usability of security tools, and considering socio-cultural factors, healthcare institutions can create an environment where compliance becomes an integral part of healthcare practice. As the healthcare sector increasingly relies on digital systems and sensitive patient data, our research underscores the critical need to fortify information security measures. This study not only contributes to the understanding of compliance behavior but also provides a roadmap for healthcare organizations striving to safeguard patient information and ensure the integrity of their operations.

B. Recommendations

Based on our study's findings, we present a series of suggestions for improving information security policy compliance among healthcare professionals working in a private hospital in Mogadishu, Somalia. These suggestions are made with healthcare organizations, legislators, and future research projects in mind.

➢ *Recommendations for Healthcare Institutions*

- Comprehensive Training Programs: The creation and implementation of thorough information security policy training programs should be a top priority for healthcare facilities. Healthcare professionals' awareness and expertise of data security procedures should be improved by these initiatives.
- Clear Communication: To properly communicate the significance of information security policy compliance, effective communication tactics should be used. Healthcare facilities should make sure that every employee is aware of the dangers and repercussions of non-compliance.

- Foster a Culture of Compliance: Institutions should work to create a culture where information security compliance is integrated into daily operations rather than just being a legal requirement. This can be accomplished with the help of the leadership and repeated reminders of the need of compliance.
- Resource Allocation: To assist compliance initiatives, adequate technological and human resources must to be allotted. To guarantee that policies are followed, healthcare facilities should make security tool investments and staff appropriately.
- Recognition and Rewards: Implement recognition and incentive programs to recognize and motivate healthcare employees who consistently show a commitment to following information security policy. Certificates and new possibilities for professional growth are two examples of recognition.

➢ *Recommendations for Policy Makers*

- Policy Framework Enhancement: The threat landscape is constantly changing, thus policymakers should examine and improve information security policy frameworks on a regular basis. Policies should be sensible, understandable, and suited to the particular requirements of the healthcare industry.
- Regulatory Oversight: To guarantee that healthcare facilities follow information security rules, think about implementing regulatory oversight and enforcement measures. This framework can include compliance checks and fines for noncompliance.
- Information Sharing: Encourage cooperation and information exchange between healthcare organizations to develop a unified strategy to data security. Encourage the exchange of best practices and knowledge gained from effective compliance initiatives.

➢ *Recommendations for Future Research*

- Cross-Cultural Studies: Future studies can look into how cultural variations affect adherence to information security policies. Comparative research across several cultural contexts might offer insightful information.
- Impact of Emerging Technologies: Examine how emerging technologies, such as telemedicine, electronic health records, and IoT devices, are affecting how people in healthcare environments adhere to information security policies.
- Longitudinal Studies: Conduct longitudinal research to evaluate the compliance behavior's long-term viability and the changing variables impacting compliance over time.
- Effectiveness of Incentive Programs: study of how well compliance with information security policy is promoted and maintained using incentive programs like recognition and awards.

VIII. FUTURE RESEARCH DIRECTIONS

In this subsection, we outline potential directions for future research in this field. Building upon the limitations and gaps identified in our study, we suggest areas that warrant further investigation, guiding researchers in advancing the knowledge base.

Our study opens the door to several promising avenues for future research in the field of information security policy compliance behavior within healthcare settings. First and foremost, there is a need for further exploration into the evolving landscape of information security threats and technologies. Future studies can delve deeper into the specific challenges healthcare institutions face in adapting to emerging threats, as well as the role of cutting-edge technologies such as Artificial Intelligence and Block chain in enhancing information security.

Research focusing on the comparative analysis of information security policy compliance across various healthcare contexts and regions would provide valuable insights. Investigating how compliance behavior varies in diverse healthcare environments, both globally and within Somalia, can shed light on the influence of contextual factors and regulatory frameworks. Additionally, longitudinal studies tracking the long-term impact of information security interventions and strategies could offer insights into the sustainability of compliance behavior. Lastly, exploring the intersection of information security compliance and patient outcomes could be a fascinating area of inquiry, uncovering the potential links between secure data practices and the quality of healthcare delivery. These future research directions can contribute to a deeper understanding of information security within healthcare and drive continuous improvement in safeguarding patient data and healthcare operations.

REFERENCES

[1]. Adan Damey, M., & Dhaka, in. (2019). *Article in International Health.*

[2]. Ahmed, Y., Naqvi, S., & Josephs, M. (2019). Cybersecurity Metrics for Enhanced Protection of Healthcare IT Systems. *International Symposium on Medical Information and Communication Technology, ISMICT, 2019-May*. https://doi.org/10.1109/ISMICT.2019.8744003

[3]. Alanazi, S. T., Anbar, M., Ebad, S. A., Karuppayah, S., & Al-Ani, H. A. (2020). Theory-based model and prediction analysis of information security compliance behavior in the Saudi healthcare sector. *Symmetry*, *12*(9), 1–21. https://doi.org/10.3390/SYM12091544

[4]. Ali, B. J., Saleh, P. F., Akoi, S., Abdulrahman, A. A., Muhamed, A. S., Noori, H. N., & Anwar, G. (2021). Impact of Service Quality on the Customer Satisfaction: Case study at Online Meeting Platforms. *International Journal of Engineering, Business and Management*, *5*(2), 65–77. https://doi.org/10.22161/ijebm.5.2.6

[5]. AlKalbani, A., Deng, H., Kam, B., & Zhang, X. (2017). Information Security Compliance in Organizations: An Institutional Perspective. *Data and Information Management*, *1*(2), 104–114. https://doi.org/10.1515/dim-2017-0006

[6]. Alotaibi, F., Furnell, S., Stengel, I., & Papadaki, M. (2019). *A Review of Using Gaming Technology for Cyber-Security Awareness University of Applied Sciences Karlsruhe , Germany*. *6*(2), 660–666.

[7]. Approach, S. (2016). pdf Research Methods For Business : A Skill-Building Approach Uma Sekaran , Roger Bougie - download pdf free CLICK HERE TO DOWNLOAD. *Sekaran Dan Bougie*.

[8]. Bidwell, P., Laxmikanth, P., Blacklock, C., Hayward, G., Willcox, M., Peersman, W., Moosa, S., & Mant, D. (2014). Security and skills: The two key issues in health worker migration. *Global Health Action*, *7*(1). https://doi.org/10.3402/gha.v7.24194

[9]. Bosnjak, M., Ajzen, I., & Schmidt, P. (2020). The theory of planned behavior: Selected recent advances and applications. *Europe's Journal of Psychology*, *16*(3), 352–356. https://doi.org/10.5964/ejop.v16i3.3107

[10]. Chin, Amita; Jones, Beth; Little, P. (2021). *A Comparative Analysis of Smartphone Security Behaviors and Practices Amita Chin Virginia Commonwealth University , United States Beth Jones Western Carolina University , United States Philip Little*. *17*(3), 57–80.

[11]. Christofidis, M. J., Hill, A., Horswill, M. S., & Watson, M. O. (2013). A human factors approach to observation chart design can trump health professionals' prior chart experience. *Resuscitation*, *84*(5), 657–665. https://doi.org/10.1016/j.resuscitation.2012.09.023

[12]. Cooper, D. R., Schindler, P. S., & Sun, J. (2006). Business research methods (Vol 9). In *Business Research Methods* (Issue 2000, p. 38). http://130.209.236.149/headocs/31businessresearch.pdf

[13]. Cooper, D. R., & Schindler, P. S. (2014). *EBOOK: Business Research Methods - Boris Blumberg, Donald Cooper, Pamela Schindler - Google Books*. https://books.google.so/books?hl=en&lr=&id=9sovEAAAQBAJ&oi=fnd&pg=PA1&dq=Cooper+and+Schindler+(2014)+&ots=2C131-IcqA&sig=u68AGDK84g_lAJkC2gQ4OF7_jl4&redir_esc=y#v=onepage&q=Cooper and Schindler (2014)&f=false

[14]. Grandgirard, J., Poinsot, D., Krespi, L., Nénon, J. P., & Cortesero, A. M. (2002). Costs of secondary parasitism in the facultative hyperparasitoid Pachycrepoideus dubius: Does host size matter? *Entomologia Experimentalis et Applicata*, *103*(3), 239–248. https://doi.org/10.1023/A

[15]. Hartnell, C. A., Ou, A. Y., & Kinicki, A. (2011). Organizational Culture and Organizational Effectiveness: A Meta-Analytic Investigation of the Competing Values Framework's Theoretical Suppositions. *Journal of Applied Psychology*, *96*(4), 677–694. https://doi.org/10.1037/a0021987

[16]. Hashi, M. J., & Isa, K. (2015). *Community Participation and Health Service Delivery in Mogadishu Municipality- Somalia*. 100–111.

[17]. Hodgkinson, G. P., & Clarke, I. (2007). *Conceptual note Exploring the cognitive significance of organizational strategizing: A dual-process framework and research agenda*. https://doi.org/10.1177/0018726707075297

[18]. Houghton, C., Meskell, P., Delaney, H., Smalle, M., Glenton, C., Booth, A., Xhs, C., Devane, D., Lm, B., Houghton, C., Meskell, P., Delaney, H., Smalle, M., Glenton, C., Booth, A., Xhs, C., Devane, D., & Lm, B. (2020). Infectious diseases : a rapid qualitative evidence synthesis. *Cochrane Database of Systematic Reviews*, *4*, CD013582. https://doi.org/10.1002/14651858.CD013582.www.cochranelibrary.com

[19]. Humaidi, N., & Balakrishnan, V. (2015a). Leadership Styles and Information Security Compliance Behavior: The Mediator Effect of Information Security Awareness. *International Journal of Information and Education Technology*, *5*(4), 311–318. https://doi.org/10.7763/ijiet.2015.v5.522

[20]. Humaidi, N., & Balakrishnan, V. (2015b). The Moderating effect of working experience on health information system security policies compliance behaviour. *Malaysian Journal of Computer Science*, *28*(2), 70–92.

[21]. Hussein, R., Karim, N. S. A., & Hasan Selamat, M. (2007). The impact of technological factors on information systems success in the electronic-government context. *Business Process Management Journal*, *13*(5), 613–627. https://doi.org/10.1108/14637150710823110

[22]. Kim, S. S., & Kim, Y. J. (2017). The effect of compliance knowledge and compliance support systems on information security compliance behavior. *Journal of Knowledge Management*, *21*(4), 986–1010. https://doi.org/10.1108/JKM-08-2016-0353

[23]. Mars, M., & Scott, R. E. (2010). Global e-health policy: A work in progress. *Health Affairs*, *29*(2), 239–245. https://doi.org/10.1377/hlthaff.2009.0945

[24]. Mburu Kimani, J., & Moi, E. (2022). DETERMINANTS OF QUALITY OF HEALTHCARE DELIVERY IN DEVOLVED SYSTEMS: CASE STUDY OF LAMU COUNTY, KENYA. *International Academic Journal of Arts and Humanities |*, *1*(3), 85–101. https://iajournals.org/articles/iajah_v1_i3_85_101.pdf

[25]. Narayana Samy, G., Ahmad, R., & Ismail, Z. (2010). Security threats categories in healthcare information systems. *Health Informatics Journal*, *16*(3), 201–209. https://doi.org/10.1177/1460458210377468

[26]. Number, W. H. O. R. (2014). *Somali Community Health Strategy*. https://www.somalimedicalarchives.org/archive/publications/429-somali-community-health-strategy-2015

[27]. Ranta, P. (2010). *Information and Communications Technology in Health*.

[28]. Vance, A., Siponen, M., & Pahnila, S. (2012). Motivating IS security compliance: Insights from Habit and Protection Motivation Theory. *Information and Management*, *49*(3–4), 190–198. https://doi.org/10.1016/j.im.2012.04.002

[29]. Warsame, A., Handuleh, J., & Patel, P. (2015). *Prioritization in Somali health system strengthening: a qualitative study*. https://doi.org/10.1093/inthealth/ihv060

[30]. Wiederhold, B. K., & Reality, V. (2015). *Journal of CyberTherapy & Rehabilitation, Volume 1, Issue 2, 2008*. *1*(2).

[31]. Yusoff, M. S. B., Arifin, W. N., & Hadie, S. N. H. (2021). ABC of questionnaire development and validation for survey research. *Education in Medicine Journal*, *13*(1), 97–108. https://doi.org/10.21315/EIMJ2021.13.1.10

[32]. Zomboko, F. E., Tripathi, S. K., & Kamuzora, F. K. (2012). Challenges in Procurement and Use of Donated Medical-Equipments: Study of a Selected Referral Hospital in Tanzania. *Journal of Arts, Science & Commerce*, *4*(4), 41–48. https://doi.org/10.13140/RG.2.2.25895.09125