JOURNAL OF POLITICAL STABILITY ARCHIVE

Online ISSN: 3006-5879 **Print ISSN:** 3006-5860

DOI: https://doi.org/10.63468/jpsa.4.3.10

Vol. 4 No. 3 (2026)

https://journalpsa.com.pk/index.php/JPSA/about

Recognized by: Higher Education Commission (HEC), Government of Pakistan

Security Policy Interpretation and Compliance Behavior Among Non-Technical Healthcare Staff

Awon Ibrahim Raza Jaffery *

MSc Cyber Security Research Scholar, School of Computing and Digital Technologies, Sheffield Hallam University, United Kingdom

airjlhr2022@gmail.com

* Corresponding Author

ABSTRACT

Healthcare organizations have information security policies that are formal rules and procedures aimed at protecting sensitive patient data, providing confidentiality, and preventing cybersecurity threats. Even with the presence of such policies, non-technical healthcare workers usually find it difficult to read and understand them properly, which exposes a level of institutional security vulnerability of information. The paper explores the way in which non-technical employees perceive, read, and execute the security policies, as well as addresses the determinants of compliance behavior, such as individual cognitive factors (e.g., self-efficacy, perceived severity), organizational culture, management support, training programs, and technological usage. The study employs a qualitative approach, summarizes the results of the empirical studies, systematic reviews, and focus groups analyses to establish the patterns of policy interpretation and compliance. The findings indicate that correct interpretation of security policies which is supported by awareness programs and organizational supportive structures plays a great role in increasing the compliance behavior and improper interpretation or lack of awareness training fosters non-compliance practices. The results of the study present suggestions to healthcare administrators and policymakers on how to create specific training, incorporate technological assistance, and establish an organizational culture that is security-based and inspires appreciation and compliance with the policies. The study can be used to add to the theoretical and practical knowledge of human factors in healthcare information security by providing a framework of how to increase policy compliance among non-technical staff.

Keywords: human organization, cognitive factors, qualitative method, security policies, theoretical knowledge

INTRODUCTION

The healthcare organizations all over the world have to make an effort to work in the highly complex environment where the security of sensitive patient information is not only a legal but also an ethical requirement. The amount of personal health information that is being processed on a daily basis coupled with disjointed workflows and a variety of employee functions imposes a lot of vulnerability in the event that security policies are not well comprehended and applied on a regular basis. According to Kwon and Johnson (2013), even written security policies in healthcare will not be effective, they need to be understood and interpreted by every member of staff and translated into actual protective behavior (Kwon and Johnson, 2013). Their paper points out that most organizations spend huge amounts of money on technical security architectures (firewalls, encryption, access controls) but severely under invest in the organizational practices that enable non-technical human beings to internalize and implement security norms. To the non-technical health care workers including the medical receptionist, billing clerks and administrator assistants, the policies usually comes in form of thick paper full of technical jargon that does not fit the day-to-day decision making scenario presented to them. This disjuncture between the organizational level of policy formulation and the user level of policy interpretation is one of the factors that lead to inconsistent compliance behaviour, increasing the risks associated with unauthorized access, accidental disclosure and regulatory non-compliance. The context of the organization therefore preconditions the recognition of the importance of staff behavior that is not related to technical issues and the role of interpreting the policies, which is as vital as their presence.

Personal Behavioral Distinguishing Factors of Security Compliance

A growing body of literature shows that personal attitude, beliefs, and personal risk evaluation are among the factors that play a significant role in determining the adherence to information security policies among healthcare workers. In a thorough review of empirical research on security behavior in health information systems, Sari, Handayani, Hidayanto, Yazid, and Aji (2022) discovered that individual attitudes towards compliance, self-efficacy in the use of security measures, and the perceived severity of threat are the personal factors that dominate in the reaction of the staff to security requirements (Sari et al., 2022). In healthcare, non-technical employees may be faced with the security requirements in the situations that seem peripheral to their major job responsibilities, i.e., filling out forms, patient admissions, or medical records. These activities are often planned on a timetable and may reduce attentiveness to security detail and likelihood of shortcuts or rule breaches. According to the review of Sari et al. there are individual proclivities to security behaviour that are not consistent; they mingle with job demands, personal conviction regarding the significance of security and the perception in which policies are expressed. This view

defines security compliance not as an organizational requirement, but as behavioral consequences, which are organized depending on individual mental models, which differ among job titles and degrees of technical acquaintance.

Non Technical Staff Security Awareness and Education

One of the main themes of cybersecurity studies in healthcare is the importance of security awareness and special education in determining compliance behavior by unofficially trained employees. In a study by Alhuwail, Al-Jafar, Abdulsalam, and AlDuaij (2021), the research revealed that healthcare professionals with a high level of information security awareness had a higher level of secure behavior than those with low awareness, and those with low awareness showed the tendency to act in a way that went against policy intents (Alhuwail et al., 2021). Their study found that there was an alarming difference in understanding between technical employees who typically get formal cybersecurity training and non-technical employees who at the most get brief orientations on security. To demonstrate, administrative staff may have no knowledge of terms like phishing, use of secure passwords, or data classification policies, but must deal with forms, patient identifiers, or software on a network that contains sensitive data. The outcome is compliance gap, which is not caused by unwillingness to pay attention to the policy but by absence of meaningful understanding of the purpose of the policy, its interpretation in work and consequences of non-adherence. Alhuwail et al. believe that role-based, structured awareness campaigns targeted at non-technical employees are necessary in order to develop security culture and convert abstract policies into behaviors that can be put into practice.

Behavioral Frameworks of Policy Interpretation and Compliance

Behavioral science can be used to provide sound models to understand why individuals choose to adhere, disregard or redefine security policies, and these findings are increasingly utilized in cybersecurity studies to understand compliance behavior in healthcare settings. Al Toobi (2025) incorporates the aspects of the Protection Motivation Theory (PMT) and the Theory of Planned Behavior (TPB) to understand how individuals (and those with limited technical background, in particular) review security policies, evaluate the perceived threats, and take action based on protective motivations (Al Toobi, 2025). Based on this framework, compliance decisions are not necessarily rational calculations but are influenced by perceived seriousness of dangers, perceptions on the effectiveness of precautionary actions, and personal convictions in keeping up with the required actions. As a non-technical healthcare employee, these cognitive and motivational variables are especially conspicuous: the lack of knowledge about the security terminology or the inability to interpret the policies correctly in case of a potential threat or the falling back to un-secure behavior in stressful situations. Behavioral theories render the process of policy interpretation dynamic and psychologically oriented, as individuals believe and social settings shape its perception as an active process instead of a passive one. According to the work by Al Toobi, the improvement of compliance intervention must take into account cognitive mechanisms by which people make

sense out of policies and, therefore, develop the messaging and training based on behavioral inclinations, not on technical considerations of the matter.

The Consequence Practicals of Incompliance of Non-Technical Security Non-Compliance

The practical consequences of policy interpretation and compliance through non-technical staff are immense and not restricted to scholarly knowledge on quantifiable operational damages. The incident with SingHealth data breach in Singapore in 2018 is one of the most publicized examples that demonstrate how the lapse in the simplest security behavior due to both training and awareness gaps may result in massive unauthorized access to patient records and subsequent publicization (Wikipedia contributors, 2019). Probes into the intrusion showed that however elaborate the policies were the same was not interpreted and enforced by all employees, especially those who lacked technical skills. The consequences of this breach were regulatory fines, a damaged reputation, and a significant operational expense to address technical vulnerabilities and lack of training in the organization. These cases point to the fact that security compliance is not an idealized concept but a practical requirement, where the failure of non-technical employees to interpret correctly can increase the threat to patient privacy, institutional credibility, and legal compliance. The practical implications of these implications highlight the need to study the behavior of non-technical personnel in relation to policies, compliance choices, and how organizational cultures can be designed to encourage behavior that leads to meeting security goals.

Human Behavior as a Security Vulnerability Causative Factor in Healthcare Workplaces

Practices of workers are critical towards defining how effective security policies can be in the medical settings, particularly among the non-technical workers whose daily work is likely to be engaged with confidential health information systems with no official skills in cyber security. According to research by Nayak, Jain, and Kemothi (2023), simple aspects of work like workload, stress, and insufficient organizational support may cause the worsening of risky security behaviors in healthcare workers, resulting in the increased vulnerability of medical systems (Nayak, Jain, and Kemothi, 2023). According to their empirical results, non-technical staff pressured and not knowing the expectations on security can use the insecure shortcuts to save time, which may include repeatedly not changing their passwords, not heeding phishing messages, or even sharing their log in details, which indirectly undermine the security in the system, and may contradict formal policy requirements. In addition, this study outlines the significance of personality factors including conscientiousness and agreeableness in influencing security practices by stating that compliance practice is not merely determined by the existence of policies, but its internalization into organizational norms by individuals. Placing non-technical personnel in the framework of the socio-psychological nature of healthcare work, the study indicates that the behavior of employees is one of its primary vulnerabilities in terms of cybersecurity in healthcare and requires specific behavioral

responses rather than only technical ones.

Antecedents of Information Security Behavior, Organizational and Individual

An increasing body of systematic literature reviews offers extensive information on antecedent means that determine information security behavior in the case of healthcare staff, including non-clinical staff. To determine which factors at an individual (e.g., self-efficacy, perceived severity of threats) and organizational (e.g., managerial support, cues to action) level shape the likelihood of securing the system, Sari, Handayani, Hidayanto, Yazid, and Aji (2022) conducted a systematic review of 35 empirical studies and found out that individual psychology (e.g., self-efficacy, perceived severity of threats) and organizational culture (e.g., managerial support, cues to action) significantly Their review points out that although most studies have focused on clinical staff, non-clinical and administrative staff have equally been subjected to influence of these antecedent factors but they have been underrepresented in studies that aim to instil secure behavior. This body of work, by identifying the interplay between factors like attitudes toward security policies, personal belief system, and organizational enforcement mechanisms, can serve to help shed light on the integrative concept of factors that can encourage non-technical employees to deviate when it comes to compliance with security policies. According to this literature, holistic security measures should be based on both psychological and structural factors in order to be effective in altering the behavior and facilitating normative conceptualization of policy demands in all healthcare positions.

Non-Compliance to Compliance Transformation: Motivational and Cultural Influences

Compliance of information security is not a fixed-state but a behavioral change that is dynamically shaped by the motivational and cultural aspects of organizations. The systematic review by Ali, Dominic, Ali, Rehman, and Sohail (2021) on information security behavior and policy compliance focuses on how employees turn their non-compliance behavior to a compliant one (Ali et al., 2021). Their discussion highlights that compliance behavior is not only influenced by the enforcement and deterrence mechanisms but it is also influenced by the intrinsic motivation by the employees (e.g., personal values and inner security awareness) and extrinsic motivation (e.g., organizational culture and support on behalf of the senior leadership). In the healthcare setting, where non-technical personnel might lack significant technical training, these motivational and cultural factors can be regarded as particularly acute: non-technical employees who feel that their fellow employees and managers provide meaningful social support or who learn company values about privacy are more susceptible to adhere to the security policies. Notably, this study indicates the effect of the organizational culture in supporting the normative interpretation of the security policies, in the sense that, it converts the abstract regulatory requirements to accepted ways of workplace practice, which are compatible with the self-concepts and social identity of the employees. In this way, closing compliance gaps necessitate a realization of the fact that it is not enough to grasp technical requirements but also the way motivational systems and workplace

cultures affect the daily-decisions of non-technical employees.

Non-Technical Compliance is One of the Parts of the Wider Healthcare Security Failures

Failure of security in healthcare is often identified as a result of human factors as non-compliance and ignorance as opposed to a technical weakness as opposed to a technical weakness, and it is important to put policy interpretation into the context of larger organizational practices. According to the latest studies on the failure of health data protection, the non-compliant behavior and the lack of cybersecurity mindfulness are rated as the major factors contributing to breaches, and some scenarios where the non-technical healthcare personnel accidentally share information due to bad practice or poor understanding of the policy intentions (Hassandoust, Techatasanasoontorn, and TanA, 2024). This study expresses that non-technical compliance is not a single event but is indicative of more profound systemic issues, such as workflow pressures, insufficient training, conflicting clinical priorities that undermine security work, and so on. To provide some examples, such automatic logout policies as putting the actual policy into effect can be bypassed or disabled by clinical throughput-focused staff, which demonstrates how a perceived operational cost can affect the interpretation of policy. Under this light, non-compliance is not just simply a question of the intentional ignorance but is intertwined with organizational anticipations, funding limits and real-life assessments of policy applicability among frontline personnel. These results support the idea that the interpretation and implementation of security policies by non-technical employees should be viewed as the key to responding to more extensive security failure trends rather than adherence to regulatory requirements.

Statement of the Research Problem

The behavior of compliance is often negatively influenced by the fact that the non-technical healthcare staff tends to misunderstand or fail to consistently comprehend the organizational security policies. Empirical literature and focus group evidence show that despite the existence of policies, staffs might have difficulties in the translation of abstract policy language to actionable and safe practice because of the lack of awareness, insufficient training, and perceived complexity of the implementation. Such a misunderstanding results in the non-compliant behavior like handling patient data improperly, bypassing system security controls, or not following standard procedure that further exposes patients to security breaches in healthcare facilities. Thus, the main research issue is the connection between policy interpretation and compliance behavior, which is what necessitates the necessity to comprehend how non-technical employees perceive, internalize, and put security measures into practice.

Research Objectives

- To investigate the perception of organizational security policies by non-technical staff in healthcare facilities, and the determinants of this perception.
- To determine the compliance behavior of non-technical healthcare personnel towards organizational security policies and the cognitive, behavioral and

organizational determinants that influence compliance.

- To examine the association between interpretation of security policy and adherence behavior to the security policy by non-technical healthcare employees in healthcare organizations.

Research Questions

1. What is the perception of the non-technical healthcare personnel towards the organizational security policies and what determines their perception?
2. What is compliance behavior in non-technical healthcare personnel and how cognitive, behavioral and organizational antecedents influence conformity to security policies?
3. What is the impact of the interpretation of security policies on compliance behaviour by non-technical healthcare employees in the healthcare organization?

Significance of the Study

The research is important as it sheds a light on the more important aspects of behavior and organizational processes that affect information security compliance in the case of non-technical healthcare personnel. The study reveals that self-efficacy, perceived threat severity, and organizational support structures are the forces behind secure behavior (Sari et al., 2022; Arif et al., 2025). These lessons can be useful to hospital administrators, healthcare managers, and policymakers in the planning of specific interventions, including role-based training schemes, better communication strategies in the policy, and incorporation of security awareness programs into routine workflows. By learning the way non-technical employees perceive policies, one can help organizations to decrease implementation gaps, decrease the potential threat of security breaches, and keep the sensitive patient data secure.

Also, the research provides an academic and practical insight as it provides a combination of empirical evidence in secondary sources with theoretical frameworks like Protection Motivation Theory (PMT). The research provides a framework that could inform future research and organizational interventions by demonstrating that perceived severity, self-efficacy and response efficacy are related to compliance behavior (Al Toobi, 2025; Ifinedo, 2012). The results emphasize the need to match policy wording, organizational culture, and technological applications with the understanding of staff and their usefulness. Consequently, the study does not only contribute to improving the rate of compliance in healthcare institutions, but it also adds value to the academic knowledge on human factors of cybersecurity in the complex healthcare systems.

Delimitation

The research is confined to non-technical health employees, including the administrative staff, receptionists, and medical assistants, without IT or technical specialists as the research is aimed at the perception and implementation of security policy by individuals with less technical skills. Moreover, the study is based on secondary data sources solely, consisting of peer-reviewed journal articles, organizational reports, and previous empirical research done . This limitation is meant

to ensure that the study gains behavioral and organizational facets of the security policy interpretation process without direct primary data gathering and to recognize that result may not necessarily be applicable to the technical employees and institutions that were not included in the studies that were examined.

LITERATURE REVIEW

Among the fundamental strands of current information security studies, it is possible to single out the behavioral factors that affect adherence to information security regulations in the healthcare personnel. The results of the studies based on behavioral theories like Protection Motivation Theory (PMT) indicate that perceived severity of threats, perceived vulnerability, and response efficacy are potent predictors of secure behavior among healthcare staff that includes non-technical personnel. As an example, the empirical study by PMT (as reported by Al Toobi et al., 2025) has shown that the perceived severity and response efficacy are major predictors of secure practice adoption, meaning that, once healthcare workers are familiar with the severity of the security threats and their belief in the usefulness of the protective measures, they tend to adhere to the policies (Al Toobi, 2025). This is in accordance with the results of Sari, Handayani, Hidayanto, Yazid, and Aji (2022), who in their systematic pool of evidence on how behavioral factors are influenced in security in health information systems found that self-efficacy and attitudes are individual antecedents that have a substantial influence on compliance behavior in different healthcare settings (Sari et al., 2022). In the same manner, studies using General Deterrence Theory and PMT (Alharbi and Alkhalifah, 2025) established that ambivalent threats of cybersecurity and coping appraisal also affect cybersecurity behavior in healthcare workers during a digital transformation, highlighting that psychological determinants are not limited to technical knowledge but perceived consequences and coping skills (Alharbi and Alkhalifah, 2025). Collectively, these two studies emphasize the fact that personal cognitive and motivational determinants play the important role in influencing information security compliance behaviors in healthcare settings, especially among personnel with informal training in technical aspects of the field.

Contribution of Awareness, Culture and Training on the Compliance of Policies

An extensive theoretical literature focuses on the importance of security awareness, organization culture, and training programs as the fundamental enablers of compliance with policies in healthcare organizations. A systematic review of information security policy compliance studies by Ahmed and Abas (2024) has shown that awareness and culture are some of the factors that can be used to influence the security behaviour of employees, and that companies with well coded security cultures and strong awareness programs are more likely to have higher levels of compliance (Ahmed & Abas, 2024). Likewise, Sari et al. (2022) systematic literature review has also defined different types of organizational antecedents, such as management support and cues to action, as existential to contribute to compliant behavior in the framework of health information systems, stating that organizational

practices should support the secure behavior in a consistent manner, to overcome human-centric risks (Sari et al., 2022). To make matters worse, empirical research such as the one undertaken in a local hospital in Mogadishu established that compliance behavior among healthcare workers is highly dependent on the effectiveness of communication and training programs as well as sociocultural factors and indicated that usability of security tools and sociocultural beliefs can either support or undermine compliance to policy (Aweis, Isak, and Mohamud, 2024). All these strands of diverse literature culminate in the perception that compliance does not come automatically, but it can be developed through consistent awareness creation and training programs, and that is particularly true with respect to meeting the requirements of the non-technical healthcare personnel.

Human Dynamic and Organization Impact on Security Factor

In addition to personal thinking and education, the recent studies have also emphasized the human and organizational-wide aspects, which can affect the behavior of security compliance within healthcare organizations. Kumar and Suri (2025) in their review of human factors impacting cybersecurity identified that human vulnerabilities, including vulnerability to social engineering, insufficient training, and weak security culture, are some of the most common contributors of breaches in the health care environment and that internal human vulnerabilities are to be considered when communicating a comprehensive security compliance strategy (Kumar and Suri, 2025). The review by Sari et al. (2022) also highlights organizational factors such as management support and cultural norms as antecedent factors directly determining secure behavior, which clarifies the importance of organizational environment and governance structures directed at how non-technical personnel interprets and implements the security policies (Sari et al., 2022). In addition, the recent studies in the sphere of digital transformation by Alharbi and Alkhalifah (2025) combine both personal and organizational factors, showing how privacy, trust, and awareness and interact with complexity of digital systems to change cybersecurity behaviour of employees in health care (Alharbi and Alkhalifah, 2025). Taken together, these researches indicate that both human and organizational aspects of security are not separable at all; they are systems-type ecosystems requiring cultivation to get significant levels of adherence to policy.

Technology, Governance and Policy Compliance Interplay

Although the literature has given a lot of attention to human and organizational antecedents, studies have also looked at the interaction of technological and governance structures with user behavior in managing compliance in healthcare facilities. According to recent integrative reviews on information security policy compliance, it is noted that technological settings, such as multi-faceted EHR systems, access controls, and pressures associated with digital transformation, cannot be separated into compliance outcomes of a human character, since they determine user experiences and perceived burdens of enacting security practices (Crossler et al., 2026). Besides, literature that analyzes the role of governance within the healthcare cybersecurity underlines the impact of security governance

systems and control measures on employees by imposing accountability systems, transparency, and compliance incentives (Alharbi and Alkhalifah, 2025). Results of these reviews indicate that governance through regulatory alignment, risk management policies and enforcement practices may or may not facilitate behavior that is secure when well applied or may cause friction when poorly applied. With the growing digitization of healthcare systems, it is crucial to comprehend the interaction between the policy, technology, and human patterns of use to create compliance strategies that are more acceptable to non-technical employees and that minimize the occurrence of unintended lapses.

Granted Interventions and Research on Healthcare on Security Compliance

The latest study has started to examine applied interventions and practical models that are used to enhance compliance with security among healthcare employees. Studies on custom security training including motivational framing approaches to video-based training have indicated that interventions consistent with users in-built motivations may positively impact skill attainments together with conformity consequences in contrast to generic training (Patterson et al., 2025). Similarly, health care governance research also reiterates that integrating factors like deterrence systems, security consciousness and trust can develop more holistic frameworks to comprehend and facilitate secure behavior amid the digital transformation (Alharbi and Alkhalifah, 2025). Moreover, the existing analytic reviews of behavioral and technological factors affecting compliance are summarized to indicate that both aspects are to be combined to address the complexity of security threats efficiently (Crossler et al., 2026). The practical implications of these findings reveal that specific, situation-specific approaches, they should be designed to meet the needs peculiar to healthcare settings and address the needs of non-technical staff, are becoming the important means of enhancing the process of policy decoding and adherence to behavioral norms.

Human Factors and Security Compliance in Healthcare Environment

The recent literature has repeated the central focus of human factors as determining the degree of adherence to information security policies by the healthcare staff. Arif et al. (2025) study has indicated that such critical human factors like the organizational security culture, awareness, training, risk perception, and reinforcement mechanisms play a significant role in the willingness of employees to adhere to information security policies, which means that the concepts of culture and training have a positive influence on compliance behaviors in any organizational environment (Arif et al., 2025). In line with this, a focus group study in Italian healthcare facilities has determined that the awareness dimension of information security is frequently a problem among the personnel, and risky behavior and policy lapses are prevalent in practice; this indicates that knowledge diffusion and policy maturity levels of knowledge remain underdeveloped among the staff (Borghesi et al., 2024). Furthermore, the study on information security compliance in the Sri Lankan healthcare Knowledge Process Outsourcing (KPO) organizations conducted by Mahipala and Perera has also revealed that the factors like employee training and

organizational culture can be said to be critical in determining compliance behavior whereas technology and regulatory frameworks can be said to be supportive but not determinants of it (Mahipala and Perera, 2025). Collectively, these results point to the conclusion that the human-related factors, not only the policy presence, have a significant impact on defining the way non-technical healthcare workers perceive and implement security regulations.

Awareness and Predictors of Behaviour of Information Security Compliance

The success of compliance security policy implementation measures in the healthcare industry is closely associated with information security awareness and the underlying psychological predictors of behavior. In the quantitative study by Al Toobi to examine the protection motivational theory (PMT) in the context of healthcare professionals in Sultanate of Oman, the perceived severity of threats and response efficacy were identified as two of the strongest motivators explaining the predictive capacity of healthcare professionals to secure behavior, meaning that employees who perceive threats seriously and protection actions as effective are much more inclined to adhere to security policies (Al Toobi, 2025). These findings are also supported by qualitative evidence collected in healthcare settings; the staff tends to have a problem with adhering to some of the essential information security awareness dimensions, which supports the notion of informational awareness gaps being transformed into evident compliance issues (Borghesi et al., 2024). Also, according to the KPO research conducted by Mahipala and Perera, the compliance is positively associated with the information security awareness and use of Health Information Systems (HIS), which further emphasizes that the information security awareness, as well as the practical use of systems, determine the secure behavior of healthcare staff significantly (Mahipala and Perera, 2025). Taken together, these investigations indicate that the concept of awareness is not a fringe factor but one of the fundamental predictors of security compliance behavior in healthcare.

Training and Policy Implementation of Organizational Culture

There has been a wide agreement in the recent studies that organizational culture and specific training are essential elements of good information security compliance approach in healthcare. The study by Arif et al. (2025) highlights the necessity of applying the human factor aspects of training and risk perception to the policy development, and found out that organizational commitment to security culture affects behavioral compliance among the employees in a positive way (Arif et al., 2025). The focus group study by Borghesi and colleagues emphasized the fact that the healthcare staff is aware of the discrepancy between the official information security policies and the way these policies are applied in practice, as the researchers identified that the non-mature policy diffusion and the lack of specific training programs tend to result in non-compliant behavior (Borghesi et al., 2024). Moreover, the analysis by Mahipala and Perera reveals that although management commitment and organizational systems did not demonstrate any direct correlation with the levels of compliance, constant training and awareness programs did have the quantifiable positive effect on the staff compliance with security policies, which implies that the

organizational culture should be operationalized through continuous education, as opposed to the policy statements (Mahipala and Perera, 2025). These researches highlight how a robust and extensive culture of information security which is reinforced by regular and situation based training is required to convert policy awareness into long lasting compliance behavior.

Adoption and Integration of Technology and Policy Compliance

Although a significant portion of the literature is rightful in its predictions of the role of human and organizational factors, there is an equally important role of technological adoption interacting with the policy-compliant results within healthcare settings. The study of healthcare KPO contexts by Mahipala and Perera (2025) reveals that the adoption of the healthcare information systems (HIS) has a strong positive relationship with compliance behavior implying that staff is more prone to follow security measures when the technological systems are properly configured in line with the policy requirements (Mahipala and Perera, 2025). The results of the study support the idea that technology cannot be treated as a standalone entity, but it should act as a facilitator of safe procedures to those employees, who deal with digital systems on a daily basis. Equally, studies in general healthcare cybersecurity settings have brought to the fore that the fast-evolving digital ecosystems, such as interlinked EHR systems and telemedicine services, present a heterogeneous attack surface, which requires not only effective technological solutions but also user-oriented policy compliance measures (Qureshi & Koo, 2026). Though not substituting behavioral and cultural determinants, these technological aspects have a synergistic effect on policy interpretation and implementation: the compliance of staff increases when systems are seen as safe, well-integrated, and helpful to their daily working routine. Therefore, current studies show that the use of technology and the adherence to policy should be co-developed to enhance the security behavior in healthcare institutions.

RESEARCH METHODOLOGY

The study research strategy aims at investigating the meaning and implementation of organizational security policies by non-technical healthcare staff. Due to the sensitivity of healthcare data and the focus on human behaviour, instead of the technical implementation, the proposed research is a qualitative one as it strives to elaborate on the causal mechanisms, reasons, and organizational factors that influence the behaviour of compliance. The proposed methodology focuses on the need to comprehend the experiences, perceptions, and practices of the healthcare personnel and incorporates the findings of the available literature, case studies, and organizational reports. This will entail using a combination of the varied qualitative methods to generate rich and depth in both the individual and organizational aspects of policy interpretation and adherence, as opposed to trying to quantify the behavior using surveys or experiment design. The methodology enables a systematic look at the behavioral, cultural, and structural aspects influencing security compliance amid non technical personnel with a basis on the implementable recommendations that

cover the practical gaps on policy execution.

Qualitative method

The qualitative aspect of this research is mainly based on document and content analysis of secondary data as a way of comprehending the interpretation and the compliance behavior of security policy in healthcare organizations. This approach implies the consideration and analysis of the already existing academic papers, organization reports, cybersecurity principles, and policy documents published in 2020-2025 to identify themes associated with staff compliance, behavioral aspects, and organizational practice. Through document analysis the researcher is able to get the recurrent patterns, the types of non-compliance and assess the ways in which policy structures, communication techniques and organizational culture affect the behavior of the staff. The research will analyze the evidence on the qualitative data regarding the perception and implementation of security measures by non-technical staff members, as well as triangulate the results of various secondary sources to increase the credibility and reliability of information. This technique is most appropriately applied in explaining the intricate behaviors that are entrenched in an organizational setting without necessarily intervening or experimenting.

Data Collection Method

The data gathering to be used in this research is purely based on systematic methods of gathering secondary resources such as journal articles, organizational reports, policy manuals, and empirical research studies. The inclusion criteria will be the publication of the study in 2020-2025 to make sure that the results can be related to the modern problems of healthcare security and the situation of digital transformation. The academic databases, e.g., Google Scholar, PubMed, Scopus, and ScienceDirect, are also used to find the sources by using the following keywords: healthcare security policy compliance, non-technical staff behavior, information security in hospitals, and organizational culture and cybersecurity. They undergo the screening of the research to streamline the process of methodological rigor, relevancy, and focus on non-technical staff members, and extract the data on relevant themes, which are coded thematically, which identifies incidences of compliance behavior, organizational effects, and policy interpretation issues. This systematic set does not leave any data sources to play some irrelevant role in answering the research questions and developing a combined picture of compliance behavior under various healthcare settings.

Research Design

The research design employed in this study is descriptive and exploratory qualitative due to the need to examine the phenomenon of policy interpretation and compliance among non-technical healthcare employees. The descriptive part can be used to document and analyze behavior pattern and organizational practice in a much more detailed way whereas the exploratory part gives the flexibility to find the emergent themes as well as subtle clues in the literature. The research design is deep and not broad-based where the authors focus on the reasons and mechanisms of compliance behavior and not the frequency of such behavior. The combination of the

thematic content analysis and the structured coding processes make the design enable the researcher to group the data into the factors including organizational culture, training, technological context and personal motivations. The practice will provide a comprehensive view of the behaviors of policy interpretation and hence be able to generate recommendations on management practices as well as future studies in healthcare information security.

Theoretical Framework

This paper is pegged on the Protection Motivation Theory (PMT), which was formulated by Rogers (1975) and subsequently magnified in information security setting by various researchers like Ifinedo (2012) and Al Toobi (2025) to describe the behavior in cybersecurity. According to PMT, cognitive appraisal of threat and coping strategies determine the way people behave in ways that are protective to them. Among them, there are perceived severity (the degree to which a threat is perceived as serious), perceived vulnerability (how predisposed an individual is to the threat), response efficacy (how effective the protective action against that threat is believed to be), and self-efficacy (confidence that one can perform the acting) (Rogers, 1975; Al Toobi, 2025). The theory implies that individuals will engage in safe behaviors when they feel that a perceived threat is serious and protective measures recommended are understandable and feasible. PMT can be used in the given study to comprehend the interpretation and adherence of security policies to the non-technical healthcare staff. As an example, the perception of unauthorized access to patient records can be viewed as a great threat (perceived severity) and the receptionist or administrative staff member may feel vulnerable because of their lack of technical training (perceived vulnerability). When they are convinced that adherence to the password and access management policies used in the organization can adequately address this risk (response efficacy), and they are convinced that they can take the necessary measures (self-efficacy) they are more likely to act in compliance with the security policies on a regular basis. Using PMT, the work can appropriately assess the influence of cognitive perceptions, motivation and confidence on compliance the behavior to provide a model on how patterns of policy compliance can be understood and how specific training or policy redesign can be used to enhance security results (Ifinedo, 2012; Al Toobi, 2025).

ANALYSIS AND DISCUSSION

The study design based on the analysis of the present research is the comprehension of the way non-technical healthcare personnel perceives organizational security policies and what conditions determine their understanding and compliance patterns. Since healthcare settings are intricate socio-technical systems, with multi-faceted users, one needs perception (in addition to knowledge) of formal requirements, a mental understanding of risks, organizational indications, and cultural factors. There is a body of empirical research and systematic literature reviews proving that the behavior related to the information security in healthcare facilities is predetermined by the mixture of personal perceptions (self-efficacy,

attitudes, perceived severity) and organizational issues (management support, culture, and training) (Sari et al., 2022). This part examines the relevance of these factors to policy interpretation amongst non-technical employees based on studies that examine antecedent factors on behavior, information security awareness problems and the linkage of individual and organizational structures relating to cognition and behavior.

Security Policy as it is Influenced by Individual Psychological Factor Interpreted

As Sari, Handayani, Hidayanto, Yazid, and Aji (2022) state, self-efficacy, perceived severity, and attitudes are individual cognitive factors that seem to be the most common in the literature on the topic of antecedent influences on the information security behavior in healthcare settings. Their systematic review of 35 studies discovered that the three most prevalent individual contributors were self-efficacy, perceived severity, and attitudes, and it is possible to assume that the interpretation of security policies by individuals is closely connected with their personal beliefs and perceptions regarding risks and their personal capabilities to adhere to security protocols (Sari et al., 2022). That is, when non-technical healthcare workers (who think that they can successfully implement security measures (self-efficacy) and see the threats as a serious problem (perceived severity)) perceive security policies as an adequate and needed part of their job descriptions, they tend to interpret these policies as the relevant ones. The absence of these psychological drivers will make formal policies an abstract rule that will be avoided or misunderstood by staff members in their day-to-day decision-making procedures. This indicates the need to focus on internal cognitive variables in terms of enhancing the interpretation and compliance levels among non-technical employees.

Security Consciousness Problems and Policy Interpretation Loopholes

Empirical studies about awareness of information security also show that interpretation issues among health care staff exist, as even with the provision of policies, the staff tends to fail to adhere to the primary security dimensions resulting in risky behaviors. In the Italian context of the main sector of the healthcare domain, a focus group study observed that the staff struggles to adhere to the primary dimensions of ISA (Information Security Awareness), which means that the policies and awareness efforts are not properly conveyed or interpreted by the end users (Neri et al., 2024). Even though this study was a broad one, taking into account all healthcare staff, the challenges in meeting the ISA dimensions, including password management, secure data handling, and secure communication, give reason to believe that non-technical staff might not necessarily understand the intent of the policies and transfer them into safe practices. The researchers were able to conclude that current information security policies are not comprehensive since they primarily address the issue of privacy but do not consider security-related issues, which compromises the capacity of the staff to interpret and respond to them correctly (Neri et al., 2024). This highlights why effective context-specific policy communication and awareness programs to non-technical audiences are necessary.

Past Organizational and Cultural Preconditions on Interpretation

The management support, cues to action, and organizational culture are also

cited as the most common organizational factors related to the information security behavior in healthcare environments by the same systematic review by Sari et al. (2022). Such aspects can highly affect the way in which non technical staff member interpret security policies. As an example, managerial support can give organizational priorities, act as a clue that security is not a game but has to be part of the daily routine, and this way, employees will understand the policy as substance and not formalism (Sari et al., 2022). Equally, organizational culture, in terms of shared values and norms can contribute or detract to policy interpretation: in cultures where security is a part of the working expectation, staff are encouraged to interpret policy text as an actionable directive, but in cultures where immediate clinical gains are prioritized over compliance, staff are prone to view security requirement as a secondary or disruptive concern. This implies that there is no way to separate interpretation of policy by non-technical personnel and the larger cultural and managerial contexts; the policies have to be anchored by organizational norms that reinforce the wanton behaviors.

Effects of Policy Clarity and Implementation Context

A different stream of research into the behavioral response to weak policy contexts demonstrates that the quality and clarity of the security policy itself is a critical factor in interpretation. As an example, Sari, Sutanto, Handayani, and Hidayanto (2024) examined information security behavior of healthcare professionals under conditions of poorly crafted security policies and discovered that even in cases when staff members were aware of the general national policies, it did not influence the desirable Isec behavior due to the lack of clarity about organizational penalties in case of non-compliance and because the practitioners themselves did not view themselves as responsible (Sari et al., 2024). In particular, the study found that the awareness of HIS users of general national policy had an impact on the perceived severity of Isec incidents, but did not affect desirable Isec behavior because no clear consequences were identified (Sari et al., 2024). This means that policy interpretation is not only concerned with content interpretation but also interpretation of context in terms of enforcement and pertinence. Where the policy is either unclear, unenforced or not tied to work work, non-technical staff might choose to interpret the policy otherwise to bring it to compliance, which is why the policy needs to be phrased with clarity and tied to work activities and to have enforcement mechanisms which underpin the correct interpretation of the policy.

Influences of Compliance Behavior and Human Factors

Human factors and the compliance behavior is one of the key themes in the recent information security research studies as it proves that individual attributes play a crucial role in influencing the way healthcare staff follows the security policies. According to a study conducted by Arif, Badila, Warden, and Rehman (2025), quantitative analysis has found that some of these critical human elements, such as security culture, perception to risk, and risk awareness, training, and reinforcement are positively correlated with employee compliance behavior (Arif et al., 2025). The authors have discovered that the most significant predictor was security culture,

which states that when the staff feel that there is a strong supportive culture regarding security, then there is a high chance that they will adhere to the policies. This implies that compliance behavior in non technical healthcare workers is not merely a matter of information of rules but rather heavily dependent upon the supportive nature of the employee to the extent that they are integrated into a supportive environment that is security oriented. The research concludes with the fact that enhancement of human factor aspects has the potential to yield more credible and dependable compliance practices and that organizations must consider the human factors in the formulation of policies as well as the development of training interventions in an effort to improve the rates of compliance.

Technology Adoption, Awareness and Compliance

The empirical studies related to the healthcare outsourcing settings demonstrate that the awareness of information security (ISA) and technological integration are closely associated with compliance behavior. In the study of the healthcare Knowledge Process Outsourcing (KPOs) and their impact on security compliance (Mahipala and Perera, 2025), the researchers discovered that there existed positive correlations between Healthcare Information Systems (HIS) adoption and ISA with security compliance (Mahipala and Perera, 2025). Although other variables, including formal security, standards of healthcare and the role of managers, did not indicate strong statistical relationships in this particular setting, both ISA and the adoption of technology were cited as key determinants of compliance.

Awareness Programs and Organization Culture in Forming Compliance

Cybersecurity compliance systematic reviews have highlighted that organizational culture and awareness programs are key determinants of the behavior of compliance extending far beyond personal knowledge. In a 2025 systematic review, Delso-Vicente, Diaz-Marcos, Aguado-Tevar, and Garcia de Blanes-Sebastiana reported that perceived effectiveness of security measures, the top management support, and the organizational culture are the most critical factors in defining the compliance behaviors among employees (Delso-Vicente et al., 2025). The review also notes that, despite the fact that technological solutions are so vital, behavioral and organizational factors such as normative beliefs, policy attitudes, and management involvement are also important in promoting compliance. The authors elaborate that the perceived costs and benefits of compliance determines the attitudes of employees towards the latter, and it is also stated that compliance behavior is not a default, but depends on cognitive assessment of the security requirements and organizational signals (Delso-Vicente et al., 2025). This supports the finding that healthcare organizations need to instill a culture that embraces security compliance, and not just articulate the policies.

Risks in Behavior and Workflow Effect on Compliance

Perceived incompatibility between efficiency in the workflow and security safeguards is one of the obstacles that directly influence compliance behavior. The studies on the failure of these security arrangements in a healthcare setting reveal that non-compliant behavior is usually associated with inadequate awareness and

convenience-based judgments, especially in a setting that has high workload requirements or usability complexities (Kolkowska, Karlsson, and Hedstrom, 2025). Respondents in this mixed-methods research indicated that daily workflow behaviors (leaving automatic logout options on because of disruptions, using personal devices because of perceived usability challenges) are some of the non-compliant behaviors that lead to actions that could compromise security measures or cause vulnerabilities. The respondents justified that time pressures and workflow may be more important than adherence, which results in practices that circumvent policy purpose. This can be related to more general literature that indicates that compliance behavior is not merely determined by policy awareness but also by the intersection of security requirements and daily working activities as well as perceived operational costs.

Interpretation as a Predictor of Compliance Behavior

Studies have been consistent in finding that the meaning that staff attribute to security policy adopts in their real behavior of compliance since interpretation leads to perceptions of relevancy, risk and enforceability. Scoping review of drivers and barriers affecting intentions of healthcare professionals to adhere to electronic health record (EHR) privacy policy revealed that major individual perceptions such as confidence and competence to comply, perceived usefulness and fear of detection or punishment in case of non-compliance were the most commonly prevalent factors in the intention to comply with privacy and security policies (Alhassani, Windle, and Konstantinidis, 2024). According to the review authors, the drivers of compliance intention were consistently reported throughout the studies to be confidence and competence to comply, perceived ease of use, and fear that non-compliance would be detected and/or punished, as they indicate that context-related interpretation of what the policy means directly influences future behavior. This proves that interpretation as perceived capability and consequences is not independent of compliance behavior but an important determinant of compliance behavior in healthcare environment where employees have to make everyday decisions regarding security practices.

Interpretation part in creation of awareness and uptaking of safe practices

The systemic reviews of information security behavioral studies show that the interpretation of security requirements is associated with antecedent conditions that lead to secure behavior that subsequently determines compliance outcomes. In the systematic analysis conducted by Sari et al., self-efficacy, perceived severity, and attitudes, which are antecedent factors, were reported as the most common individual determinants of security behavior in healthcare settings, and they indicated that individuals tend to obey security-related policies more often when they believe they are applicable to their individual perceived threat level and personal capacity to take actions on it (Sari et al., 2022). This means that interpretation will turn abstract language in policy to personal meaning e.g. whether the non-technical staff view a policy as an element that safeguard sensitive information or a rule to avoid in order to evade bureaucracy. Moreover, the organizational aspect, including the management support, cues to action, and organizational culture, also play a role in interpretation as they indicate how serious the company takes compliance to policies,

which in turn influences behaviour. Therefore, the literature indicates that interpretation is a mediating factor of high importance that links external policy directives with internal compliance behavior.

The Interpretation, Awareness, Compliance Gaps in the Practice

The empirical studies of healthcare offer practical evidence that the gap in interpretation is associated with poor adherence behavior. The results of a qualitative study conducted by the Italian public healthcare sector on information security awareness revealed that personnel experience challenges when complying with the primary dimensions of the ISA [information security awareness], which results in risk-prone behavior (Neri et al., 2024). The analysis also noted the policy diffusion and information security awareness programs were inconsistent and undeveloped, i.e. the personnel were not always able to read between the lines and understand what the policies demanded or why, which consequently resulted into non-compliance. This research specializes in the area of awareness but it makes it clear that when people do not interpret in a correct way or have insufficient understanding of security practices, the results are suboptimal compliance behavior because employees are either not following security practices or are not following them uniformly because of misunderstanding the intent of the policies. This demonstrates that when non-technical personnel play a key role in the medical field in dealing with sensitive information, proper interpretation is the baseline in establishing believable compliance.

Perception of the salience and efficacy of compliance is determined by Policy Interpretation

Quantitative findings of studies in health care Knowledge Process Outsourcing (KPO) environments strengthen the relation between interpretation and compliance behavior by showing that the greater predictors of compliance are awareness and system adoption, which in turn is affected by how the staff interprets the policy context, rather than formal regulations per se. An analysis of healthcare KPO organizations indicated that Information Security Awareness (ISA) and adoption of Health Information Systems (HIS) reported positive significant dependency on compliance, but other factors, including managerial involvement, did not present strong dependency results (Mahipala & Perera, 2025). These findings suggest that compliance behaviour is not a product of policy presence but rather a product of staff interpretation of the utility and applicability of those policies in real-life usage and awareness situations. Once the staff believes that security instructions are important, comprehensible and in line with daily work resources such as HIS, they exhibit better behaviors of compliance. Weak interpretation does not bring about secure practices even when policies are well written.

Discussion of the Study

This study was aimed at describing the effect of security policy decoding by non-technical personnel in the healthcare environment on their compliance. These results are aligned with the current literature that indicates that the compliance of information security is not only a technical problem but a human and organizational

issue in nature. Indicatively, Sari et al. (2022) revealed that the self-efficacy, perceived severity, and attitudes of respondents are some of individual factors that impact security behavior in healthcare environments (Sari et al., 2022). This argues that the more the non-technical employees are made to appreciate the severity and applicability of security policies, as opposed to considering them as regulations, the more they demonstrate compliance. Equally, the focus group data on the Italian healthcare sector provided evidence that staff struggles to adhere to the fundamental security awareness dimensions, which also implies that the interpretation issues result in non-commitment practices, including careless data processing or the inability to adhere to the set-of-guidelines (Neri et al., 2024). In this regard compliance behavior seems to be an aspect that has a significant mediating antecedent on the way in which staffs view the meaning and the relevance of security policies in respect to their daily work tasks as opposed to the existence of the policies themselves.

The second important facet of the discussion is that the organizational culture and training programs are important to form this interpretation-compliance dynamic. Research indicates that healthcare organizations that have strong Security Education, Training, and Awareness (SETA) initiatives achieve much higher levels of compliance due to the staff being better at realizing the policies as components of organisational cultures, rather than optional extras (Mohamuda et al., 2025). There is a mediation effect between policy compliance and policy outcome such as patient privacy protection that implies that the interpretation is improved where the staff has systematically been educated about threats, consequences, and protection mechanisms (Mohamuda et al., 2025). This is in line with other literature that awareness programs are necessary in order to translate the abstract policy wording into perceived and behavioural actions (Sari et al., 2022). Moreover, the healthcare outsourcing setting research revealed that policies were more readily followed in institutions with a high level of technological use and the ISA (Information Security Awareness), which once again confirms the idea that the employment of policies according to the awareness and systems integration make them more obeyed (Mahipala and Perera, 2025). Combined, the research proves the inseparability of interpretation and compliance as a phenomenon, not independent of human and organizational processes.

CONCLUSION

This paper shows that the interpretation of security policies has a substantial effect on compliance practices of nontechnical healthcare personnel, which confirms the importance of the policies alone without considering the human factor. The literature highlights that individual cognitive factors, i.e. perception of severity, self-efficacy, and attitudes influence how the staff internalize security requirements, which subsequently influences their practice behavior (Sari et al., 2022). As long as healthcare workers cannot appropriately read the meaning or implications of security policies, they tend to follow them more rarely and with this fact a gap in the institutional protection.

Besides cognitive determinants, the conclusions have a clear indication on the significance of organizational support systems, particularly, Security Education, Training, and Awareness (SETA) program. Recent empirical studies on this topic, such as in healthcare settings, show that such programs are mediating the policy-compliant behavior relationship and boosting both interpretation and practical adherence (Mohamuda et al., 2025). It means that healthcare facilities that invest in ongoing training and sensitization efforts with a clear connection to the policy intent will result in more correct interpretation and will result in an increase in compliance levels.

Lastly, technology coupled with awareness programmes and policy models is important in promoting compliance behaviour. The results of researches on the Knowledge Process Outsourcing (KPO) setting in healthcare also indicate that compliance was strongly correlated with the adoption of information systems and awareness programs, whereas managerial involvement or organizational systems did not demonstrate as strong relationship (Mahipala & Perera, 2025). As such, healthcare institutions should also employ holistic strategies that do not just create clear policies but embrace training, technological support, and culture reinforcement practices that will make sure that the policies not only get interpreted but also put into actions.

Suggestions

To improve the security policy interpretation and compliance of the non-technical healthcare personnel, healthcare organizations must use ongoing, role-based training and awareness programs that help bind policy requirements to real-life tasks and threats. This will assist the staff to perceive the sense and applicability of the policies more precisely and convert them into uniform safe actions.

REFERENCES

Al Toobi, A. (2025). Information security behavior of healthcare professionals using a PMT model. Scientific Reports. https://doi.org/10.1038/s41598-025-26917-x

Alharbi, A., & Alkhalifah, A. (2025). Cybersecurity governance in the healthcare sector during digital transformation: An integrated model and hybrid analytical approach. Frontiers in Public Health. https://doi.org/10.3389/fpubh.2025.1703689

Alhassani, N. D., Windle, R., & Konstantinidis, S. T. (2024). A scoping review of the drivers and barriers influencing healthcare professionals' behavioral intentions to comply with electronic health record data privacy policy. Health Informatics Journal. https://doi.org/10.1177/14604582241296398

Alhuwail, D., Al-Jafar, E., Abdulsalam, Y., & AlDuaij, S. (2021). Information security awareness and behaviors of health care professionals at public health care facilities. Applied Clinical Informatics, 12(4), 924–932. https://pubmed.ncbi.nlm.nih.gov/34587638/

Ali, R. F., Dominic, P. D. D., Ali, S. E. A., Rehman, M., & Sohail, A. (2021). Information security behavior and information security policy compliance: A systematic literature review for identifying the transformation process from

noncompliance to compliance. Applied Sciences, 11(8), 3383. https://doi.org/10.3390/app11083383

Arif, M., Badila, M., Warden, J. M., & Rehman, A. U. (2025). A study of human factors toward compliance with organization's information security policy. Information Security Journal: A Global Perspective, 34(3), 235–250. https://doi.org/10.1080/19393555.2025.2457702

Aweis, Z. A., Isak, M. A., & Mohamud, A. J. (2024). Factors influencing information security policy compliance behavior: A case study of healthcare workers in a private hospital in Mogadishu. International Journal of Innovative Science and Research Technology, 9(7), 3425–3436.

Borghesi, N., et al. (2024). Understanding information security awareness: Evidence from the public healthcare sector. Information Systems Management. https://doi.org/10.1108/ICS-04-2024-0094

Crossler, R., et al. (2026). Information security policy compliance: A structured review using scientometric analysis and topic modeling.

Delso-Vicente, A.-T., Díaz-Marcos, L., Aguado-Tevar, O., & García de Blanes-Sebastián, M. (2025). Factors influencing employee compliance with information security policies: A systematic literature review of behavioral and technological aspects in cybersecurity. Future Business Journal, 11, 28.

Hassandoust, F., Techatasanasoontorn, V., & TanA, D. (2024). Towards a model for understanding failures in health data protection: A mixed-methods study. Behaviour & Information Technology.

Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. Computers & Security, 31(1), 83–95. https://doi.org/10.1016/j.cose.2011.10.007

Kolkowska, E., Karlsson, F., & Hedström, K. (2025). Towards a model for understanding failures in health data protection: A mixed-methods study. Information Security Journal: A Global Perspective.

Kwon, J., & Johnson, M. E. (2013). Security practices and regulatory compliance in the healthcare industry. Journal of the American Medical Informatics Association, 20(1), 44–51. https://pubmed.ncbi.nlm.nih.gov/22955497/

Mahipala, C., & Perera, P. (2025). Exploring information security compliant behaviors in healthcare knowledge process outsourcing (KPOs). BMC Medical Informatics and Decision Making, 25, 394. https://doi.org/10.1186/s12911-025-03007-6

Mohamuda, A., Khawa, T. A. R., & Dahir, A. (2025). Impact of information security policy compliance on protecting patient privacy: Mediating role of SETA program. Information Security Journal: A Global Perspective. https://doi.org/10.1080/19393555.2025.2542164

Nayak, P. P., Jain, K. V., & Kemothi, S. (2023). Evaluating the influence of healthcare employee behavior on cybersecurity vulnerabilities in medical systems. Seminars in Medical Writing and Education.

Neri, M., Benevento, E., Stefanini, A., Aloini, D., Niccolini, F., Federigi, I., & Dini, G. (2024). Understanding information security awareness: Evidence from the public healthcare sector. International Journal of Information Security. https://doi.org/10.1108/ICS-04-2024-0094

Patterson, E. S., et al. (2025). Motivational framing strategies in health care information security training. JMIR Medical Education.

Qureshi, R., & Koo, I. (2026). A comprehensive survey of cybersecurity threats and data privacy issues in healthcare systems. Applied Sciences, 16(3), 1511. https://doi.org/10.3390/app16031511

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. The Journal of Psychology, 91(1), 93–114. https://doi.org/10.1080/00223980.1975.9915803

Sari, P. K., Handayani, P. W., Hidayanto, A. N., Yazid, S., & Aji, R. F. (2022). Information security behavior in health information systems: A review of research trends and antecedent factors. Healthcare, 10(12), 2531. https://doi.org/10.3390/healthcare10122531

Sari, P. K., Sutanto, J., Handayani, P. W., & Hidayanto, A. N. (2024). Information security behavior of healthcare professionals when there is poor health information security policy. PACIS 2024 Proceedings.