ISSN: 2182-2069 / E-ISSN: 2182-2077

Investigating the Main Factors Affecting Healthcare Workers' Information Security Behaviors: An Empirical Study in Indonesia

Puspita Kencana Sari[1*], Nurvita Trianasari[2], and Adhi Prasetio[3]

[1*]School of Economics and Business, Telkom University, Bandung, Indonesia.
puspitakencana@telkomuniversity.ac.id, https://orcid.org/0000-0002-2679-0827

[2]School of Economics and Business, Telkom University, Bandung, Indonesia.
nurvitatrianasari@telkomuniversity.ac.id, https://orcid.org/0009-0002-8017-8740

[3]School of Economics and Business, Telkom University, Bandung, Indonesia.
adhipras@telkomuniversity.ac.id, https://orcid.org/0000-0002-4025-0237

Received: October 27, 2024; Revised: November 25, 2024; Accepted: January 04, 2025; Published: February 28, 2025

Abstract

Human factors significantly contribute to breaches in healthcare organizations, such as a lack of awareness regarding cybersecurity threats. This study aims to evaluate the information security behaviors of healthcare workers and identify critical demographic factors that influence them. The demographic factors examined in this study include age, gender, education level, type of profession, and frequently used devices to access health information systems (HIS). Information security behavior evaluated in this study consists of four dimensions: Device Protection, Password Management, Proactive Awareness, and Information Handling. This study employs quantitative methods. Data are collected through an online survey of 209 health workers in Indonesia. The data analysis process consists of two stages. The first stage is comparison group analysis using the Chi-square test to define significant factors in studied security behavior, and the second stage is multivariate analysis, which employs binary logistic regression to determine the most impactful variables. The findings show that, among the five characteristics examined, education level had the most significant effect on the information security behavior of healthcare workers in Indonesia. It underlines the necessity of education in sculpting security practices and awareness in an ever-changing digital world. This study recommends that while developing a security training and awareness program, the education level of healthcare workers should be considered to improve healthcare facilities' security posture and decrease data breach risks. As a result, governments and healthcare managers are encouraged to emphasize training programs as a strategic method of improving information security standards in the business.

Keywords: Information Security Behavior, Healthcare, Demographic Factor, Education.

1 Introduction

Health information systems (HIS) offer complete functionality, ranging from using electronic medical records (EMRs) to accessing them using web-based telemedicine. So, when such a user base, which is people and patients, allows healthcare professionals to grow with themselves, the implementation of

Journal of Internet Services and Information Security (JISIS), volume: 15, number: 1 (February), pp. 1-15.
DOI: *10.58346/JISIS.2025.I1.001*

*Corresponding author: School of Economics and Business, Telkom University, Bandung, Indonesia.

HIS should be secured and placed at the highest concern (Chang, 2015; Karimov & Sattorova, 2024). Human factors, such as ignorance of cyber threats and inadequate cybersecurity awareness, can negatively impact cybersecurity in healthcare organizations (Nifakos et al., 2021). Most security breaches in healthcare organizations are due to some form of human behavior, while the rest were initiated by outside actors (Albarrak, 2011; Alumaran et al., 2015; Deursen et al., 2013). The number of different users will make it a major target for security threats. Thus, HIS users' awareness of information security behavior (ISB) is essential to ensure proper protection.

In general, research conducted on information system security focuses on how to secure the system from the aspects of technology, process, and protocol. More sophisticated security systems require additional approaches, namely the need for employees with adequate skills to participate in securing the system by implementing security standards. This certainly involves an assessment of the knowledge and skills of health workers related to information system security (Nunes et al., 2021). HIS users are generally divided into two categories, namely health workers and patients. Previous research (Sari et al., 2023) shows that the two categories differ in user behavior. Information security threats that need to be watched out for are internal threats such as misuse and user indifference when utilizing HIS. This usually becomes more vulnerable when health workers must utilize HIS during critical situations (Verizon, 2019). Specifically, this study attempts to conduct an in-depth analysis of information security behavior for the category of HIS users from health workers. The analysis undertaken will reveal what dominant factors influence their behavior. Several studies show different results related to these factors. Several studies (Alexandrou & Chen, 2019; Fernández-alemán et al., 2015; Kessler et al., 2020; Mishra et al., 2014) show that in the case of health workers, the influence of age is an influential factor, another study (Nunes et al., 2021) show that this factor has no influence. This also occurs in studies examining gender factors where the following studies (Alexandrou & Chen, 2019) show an influence, but some (Fernández-alemán et al., 2015; Mishra et al., 2014; Nunes et al., 2021) do not show an influence. It is still relatively rare to study the education factor with varying results, especially regarding its significance level (Fernández-alemán et al., 2015; Mishra et al., 2014; Sari et al., 2024). Further research is necessary to identify the key factors influencing health workers' ISB to develop effective strategies for promoting security education and awareness (Escobedo et al., 2024).

Various studies have been conducted to reveal how to promote information security behavior effectively. However, these studies focus more on developed countries (Donalds & Barclay, 2022; Osei-Bryson et al., 2022). On the other hand, Indonesia is still in the developing country stage. Indonesia's position as a developing country aligns with the still low cybersecurity system, resulting in vulnerability to security threats (Chairil, 2019). National Cyber Security Index (NCSI) data shows that Indonesia is in 48th position in information security protection. This condition also impacts information security in the national health system (Boopathy et al., 2024). To improve national health services, the Indonesian government is continuously trying to encourage the use of HIS, one of which is promoting the use of electronic medical records through digital transformation programs and regulations in the health sector (Vanan et al., 2019). Until 2022, the Ministry of Health noted that the penetration of the use of the HIS in Indonesia had reached 88% for hospitals. Unfortunately, this is not balanced with implementing adequate information system security (Surendar, 2024). Only a few health service providers implement sufficient information security governance and infrastructure (Badan Siber dan Sandi Negara, 2020). As a result of the low implementation of existing security, many attacks on information systems are dominated by incidents such as data breaches, ransomware, and deface attacks (Badan Siber dan Sandi Negara, 2022). Several cases related to ransomware in the health sector combined ransomware and social engineering attacks by utilizing exploits sent via email

(Clementine et al., 2014). This attack depends on employee awareness and the ability to secure their systems from various attacks. Good information security behavior is the primary defense system in securing HIS.

This study aims to address this problem by examining health workers' security behavior and the primary demographic factors affecting them. The factors that are candidates in this study include the demographic characteristics of respondents, namely age, gender, education, and health profession type. Quantitative approaches are used to collect and analyze the data from health workers in Indonesia. Academically, this study is expected to contribute to empirical evidence in information security behavior research, especially in healthcare. This study will provide practical suggestions on appropriate security education strategies to increase health workers' awareness of information security.

This paper is structured into several sections. The first section details the research methods, encompassing the population and sample size, research instruments, and data analysis techniques. The following section presents the results of the data analysis, which discusses the findings, their implications, and suggestions for future research directions. The final section addresses the conclusions of this study.

2 Research Methods

Population and Sampling

Indonesia ranks the lowest on the cybersecurity index among G20 countries (Osei-Bryson et al., 2022). Many healthcare providers in Indonesia need more information security policies, primarily due to the absence of national regulations governing health information security. Despite this, the government is promoting the implementation of HIS across all healthcare facilities. By comprehending Information Security Behavior (ISB), we can take a crucial initial step toward developing more robust policies for health information security. The target population for this study consists of healthcare workers at health facilities in Indonesia. The sampling method used is non-probability sampling, specifically purposive sampling, based on the following criteria: (1) Healthcare workers with user accounts in the HIS and (2) HIS provided and managed by health facilities through web-based platforms and mobile applications.

Research Instrument

This study utilizes a modified ISB measurement scale specifically for health security risks from (Sari et al., 2023). It derived from previous frameworks namely Security Behavior Intentions Scale (SEBIS) (Egelman & Peer, 2015), Risky Cybersecurity Behaviors Scale (RScB) (Hadlington, 2017), Human Aspects of Information Security Questionnaire (HAIS-Q) (Parsons et al., 2014; Parsons et al., 2017), and Counterproductive Computer Security Behaviors (CCSB) (Ifinedo & Akinnuwesi, 2014). The information security behavior is categorized into four dimensions. These dimensions, adopted from HAIS-Q and SEBIS, include Device Protection (DP), Password Management (PM), Proactive Awareness (PA), and Information Handling (IH) (Krishnan et al., 2022). Each dimension is considered as a research variable in this study. A mapping of each item with their corresponding framework can be found in Table 1.

The questionnaire consists of two sections. The first section collects demographic information from respondents, and the second section consists of 26 items to assess health workers' behavior. The items are modified from the previous study (Sari et al., 2023), where all negative security behavior was

converted into positive security behavior. The questionnaire was distributed in Bahasa and shared through online survey platforms from April – June 2024. We employ a 5-point scale from "never" to "always."

Table 1: Information Security Behavior (ISB) Indicators in Research Instruments

Item Code	Questionnaire items	References Framework
	Device Protection	
DP1	I set my device screen to automatically lock if it is not used for a certain period.	SEBIS, HAIS-Q
DP2	I use a password/PIN to unlock my device to access the Health Information System (HIS).	SEBIS
DP3	I store the device used to access HIS in a safe place when not in use.	HAIS-Q, CCSB
DP4	I log out of HIS after I have finished using it.	CCSB
DP5	I promptly perform software updates (e.g., accepting updates or following a schedule) for my device.	SEBIS, RScB, CCSB
DP6	I do not disable the antivirus on my device to access HIS.	RScB
	Password Management	
PM1	I use a combination of letters, numbers, and symbols in the password for my HIS account.	SEBIS, HAIS-Q, RScB, CCSB
PM2	I use a different password for my HIS account than other accounts.	SEBIS, HAIS-Q, RScB
PM3	I regularly change the password for my HIS account.	CCSB
PM4	I do not share my HIS account password with friends and colleagues.	CCSB
PM5	I change the default password for my HIS account given by the administrator unless I am required to do so.	HAIS-Q, RScB, CCSB
PM6	I change the default password for my HIS account given by the administrator unless I am required to do so.	SEBIS, HAIS-Q
	Proactive Awareness	
PA1	I submit information to the website only after verifying that it will be sent securely (e.g., seeing the lock icon in the browser)	SEBIS, HAIS-Q, RScB
PA2	I ensure the mobile app I download belongs to the correct organization (e.g., a telemedicine app from the relevant healthcare facility).	SEBIS, HAIS-Q, RScB
PA3	I do not open email attachments from unknown senders.	HAIS-Q
PA4	I regularly review my social media privacy settings.	HAIS-Q
PA5	When accessing the Internet, I am cautious about visiting any websites.	SEBIS, HAIS-Q, CCSB
PA6	I only download files (e.g., software, digital music, games) from official sources.	HAIS-Q, RScB, CCSB
PA7	I use private/password-protected Wi-Fi to send sensitive information (e.g., payment information, medical resumes).	HAIS-Q, RScB
PA8	I do not share sensitive information (e.g., patient examination results) on social media.	HAIS-Q, RScB
	Information Handling	
IH1	When sensitive documents (e.g., medical summaries, prescriptions, ultrasound prints) need to be discarded, I ensure they are properly destroyed.	HAIS-Q
IH2	I do not leave documents containing sensitive information in plain sight.	HAIS-Q
IH3	I back up important files related to health examination results in the HIS.	CCSB
IH4	I handle sensitive data carefully (e.g., by entering health examination data completely and accurately).	RScB, CCSB
IH5	After verifying that the account belongs to the relevant healthcare facility, I send sensitive data for telemedicine services via instant messaging.	RScB
IH6	I do not send personal information such as health examination results to unknown websites.	RSCB

The validity test was conducted based on 30 data points from a pilot study, using Pearson Product Moment correlation and the measurements obtained via SPSS 24.0 software, with a significance level (α) of 0.05 (5%). The reliability test was carried out using internal consistency or the degree of accuracy of responses. SPSS software was employed for this reliability testing to ascertain the consistency of respondents' answers. A measurement instrument is deemed reliable and can proceed to the next stage if the Cronbach Alpha coefficient value is ≥ 0.6. Conversely, if the instrument has a coefficient value of r < 0.6, it is considered unreliable. Based on the table below, it can be concluded that all questionnaire instruments are valid and reliable because r-count > 0.300 and Cronbach Alpha value > 0.6. Table 2 shows the validity and reliability test results that imply all the items are valid and research variables are reliable for further analysis.

Table 2: Validity and Reliability Test Result

Variables	Cronbach Alpha	Item code	Pearson Correlation (r)
Device Protection (DP)	0.813	DP1	0,672
		DP2	0,798
		DP3	0,703
		DP4	0,604
		DP5	0,781
		DP6	0,786
Password Management (PM)	0.638	PM1	0,600
		PM2	0,649
		PM3	0,712
		PM4	0,631
		PM5	0,428
		PM6	0,552
Proactive Awareness (PA)	0.825	PA1	0,551
		PA2	0,854
		PA3	0,643
		PA4	0,755
		PA5	0,868
		PA6	0,708
		PA7	0,717
		PA8	0,394
Information Handling (IH)	0,775	IH1	0,713
		IH2	0,788
		IH3	0,691
		IH4	0,738
		IH5	0,552
		IH6	0,775

Data Analysis Technique

The data analysis process is conducted in two stages. The first stage involves comparing two groups of data for each demographic factor. In this study, the compared demographic factors include age (18-29 and 30-39 years), gender (male and female), education level (high school and higher education), type of occupation (medical staff and non-medical staff), and the devices used to access the Health Information System (PC/laptop and smartphone). The comparison of characteristics in categorical data is conducted by calculating the p-value based on the Chi-square test, with the alternative Kolmogorov Smirnov test and Exact Fisher test applied if the conditions for the Chi-square test are not met. A p-value < 0.05 indicates that the variable is significant statistically, suggesting a difference in information security behavior among the two groups concerning the demographic factors.

The second stage involves multivariate analysis using binary logistic regression. The demographic factors included in the first regression model as independent variables are those that had a p-value < 0.25 in the first stage. Testing is done in multiple stages according to the number of independent variables in the first model. The final model will reveal which variables strongly influence the dimensions of information security behavior.

3 Result and Analysis

We collected data from 230 respondents. We exclude the incomplete answers from the survey. After validating the data, only 209 data are continued for further processing. The demographic characteristics of respondents can be seen in Table 3.

Table 3: Respondent Characteristics

Demographic Factor		**Frequency (%)**
Age	18-29 years	166(79.4%)
	30-39 years	43(20.6%)
Gender	Male	71(34.0%)
	Female	138(66.0%)
Education Level	High School	84(40.2%)
	Higher Education	125(59.8%)
Health Profession	Medical staffs	138(66.0%)
	Non-medical staffs	71(34.0%)
Device to access HIS	PC/laptop	60(28.7%)
	Smartphone	149(71.3%)

Table 3 presents 166 healthcare workers aged 18-29 years (79.4%) and 43 healthcare workers aged 30-39 years (20.6%). Among them, 71 (34.0%) are male and 138 (66.0%) are female. Regarding education, 84 (40.2%) have completed high school, while 125 (59.8%) have higher education. The healthcare professionals include 138 (66.0%) working as medical staff, such as doctors, dentists, and nurses, who heavily interact with patient care, and 71 (34.0%) are non-medical staff consisting of another profession outside as stated in medical staff. The primary device used to access Health Information Systems (HIS) is smartphones, with 149 (71.3%) utilizing this device, while the remaining 60 (28.7%) use computers/laptops.

Table 4: Characteristics Comparison for Device Protection (DP) Behavior

Variables	**Level of DP**		**OR CI 95%**	**P-Value**
	High	**Low**		
	N=107	**N=102**		
Age			**0.703**	**0.307**
18-29	82(76.6%)	84(82.4%)	(0.357-1.385)	
30-39	25(23.4%)	18(17.6%)		
Gender			**0.946**	**0.849**
Female	70(65.4%)	68(66.7%)	(0.533-1.677)	
Male	37(34.6%)	34(33.3%)		
Education level			**2.242**	**0.005***
Higher education	74(69.2%)	51(50.0%)	(1.275-3.945)	
High school	33(30.8%)	51(50.0%)		
Profession			**1.883**	**0.032***
Medical staff	78(72.9%)	60(58.8%)	(1.053-3.365)	
Non-medical staff	29(27.1%)	42(41.2%)		
Device to access HIS			**0.551**	**0.055**
Smartphone	70(65.4%)	79(77.5%)	(0.299-1.016)	
PC/Laptop	37(34.6%)	23(22.5%)		

Table 4 presents a categorical analysis of Device Protection (DP) behaviors using the Chi-Square test, focusing on age, gender, education, occupation, and commonly used devices to access HIS. The analysis reveals that the P-values for age, gender, and frequently used devices exceed 0.05, indicating no significant differences in DP behavior among these categories. However, the P-values for education and occupation are below 0.05, suggesting substantial differences in DP behaviors between high school and higher education individuals and between medical versus non-medical workers. The Odds Ratio for education (1.275-3.945 confidence interval) shows healthcare workers with a college education are 2.242 times more likely to exhibit DP behavior than those with a high school education. Similarly, the Odds Ratio for profession (1.053-3.365 confidence interval) indicates that medical personnel are 1.883 times more likely to demonstrate DP behavior than other healthcare workers.

Following this bivariate analysis, a multivariate analysis (Table 5) examined the interplay of several independent variables to identify critical factors influencing DP behavior. Independent variables with a p-value < 0.25, including education level, profession, and frequently used devices, were included in the initial model. Results indicated that not all p-values were < 0.05, suggesting that these factors do not significantly affect HIS user behavior. Ultimately, the final model concludes that only education has a strong predictive association with Device Protection behavior.

Table 5: Multivariate Analysis for Device Protection (DP) Behavior

		B	**S.E.**	**Wald**	**P- Value**	**OR**	**CI 95%**	
							Lower	**Upper**
FIRST MODEL	Education level	0.610	0.345	3.132	0.077	1.840	0.937	3.616
	Profession	0.215	0.358	0.361	0.548	1.240	0.615	2.499
	Device to access HIS	-0.258	0.349	0.545	0.461	0.773	0.390	1.532
FINAL MODEL	Education level	0.808	0.288	7.854	0.005	2.242	1.275	3.945

Table 6: Characteristics Comparison for Password Management (PM) Behavior

Variables	**Level of PM**		**OR CI 95%**	**P-value**
	High	**Low**		
	N=95	**N=114**		
Age			**0.832**	**0.595**
30-39	18(18.9%)	25(21.9%)	(0.422-1.640)	
18-29	77(81.1%)	89(78.1%)		
Gender			**0.791**	**0.424**
Female	60(63.2%)	78(68.4%)	(0.446-1.405)	
Male	35(36.8%)	36(31.6%)		
Education level			**2.310**	**0.004***
Higher Education	67(70.5%)	58(50.9%)	(1.301-4.101)	
High school	28(29.5%)	56(49.1%)		
Profession			**1.894**	**0.033***
Medical staff	70(73.7%)	68(59.6%)	(1.050-3.418)	
Non-medical staff	25(26.3%)	46(40.4%)		
Device to access HIS			**0.583**	**0.079**
Smartphone	62(65.3%)	87(76.3%)	(0.319-1.067)	
PC/Laptop	33(34.7%)	27(23.7%)		

Table 6 shows that the P-values for age, gender, and frequently used devices exceed 0.05, indicating no statistical significance. In contrast, the P-values for education and profession are below 0.05, demonstrating statistical significance. This signifies a significant difference in password management behavior relative to education and occupation. The Odds Ratio (OR) with a confidence interval of (1.301-4.101) suggests that individuals with higher education are 2.310 times more likely to

manage passwords better than those with lower education. Additionally, the Odds Ratio (1.050-3.418) indicates that medical staff are 1.894 times more likely to excel in password management than non-medical staff.

Following the bivariate analysis in Table 6, a multivariate analysis in Table 7 investigates the relationship between several independent variables and password management behavior. The initial model includes education, profession type, and frequently used devices. The final model concludes that education is the only variable significantly associated with predicting password management behavior.

Table 7: Multivariate Analysis for Password Management (PM) Behavior

		B	S.E.	Wald	P-Value	OR	CI 95%	
							Lower	Upper
FIRST MODEL	Education level	0.663	0.349	3.607	0.058	1.941	0.979	3.850
	Profession	0.219	0.363	0.365	0.546	1.245	0.611	2.538
	The device used to access HIS	-0.183	0.344	0.281	0.596	0.833	0.424	1.636
FINAL MODEL	Education	0.837	0.293	8.179	0.004	2.310	1.301	4.101

Table 8: Characteristics Comparison for Proactive Awareness (PA) Behavior

Variable	Level of PA		OR CI 95%	P-Value
	High	Low		
	N=89	N=120		
Age			**0.963**	**0.914**
30-39	18(20.2%)	25(20.8%)	(0.488-1.900)	
18-29	71(79.8%)	95(79.2%)		
Gender			**0.980**	**0.945**
Male	30(33.7%)	41(34.2%)	(0.549-1.748)	
Female	59(66.3%)	79(65.8%)		
Education Level			**2.708**	**0.001***
Higher education	65(73.0%)	60(50.0%)	(1.502-4.882)	
High school	24(27.0%)	60(50.0%)		
Profession			**0.688**	**0.211**
Non-medical staff	26(29.2%)	45(37.5%)	(0.382-1.238)	
Medical staff	63(70.8%)	75(62.5%)		
Device to access HIS			**0.958**	**0.889**
Smartphone	63(70.8%)	86(71.7%)	(0.523-1.755)	
PC/Laptop	26(29.2%)	34(28.3%)		

The Chi-Square statistical test in Table 8 revealed that the variables of age, gender, profession, and commonly used devices were not statistically significant ($P > 0.05$). In contrast, the education variable had a P value of less than 0.05, indicating a statistically significant relationship with Proactive Awareness behavior. Specifically, the Odds Ratio (1.502-4.882) showed that healthcare workers with a higher education level (Diploma, Graduate) were 2.708 times more likely to exhibit Proactive Awareness behavior than those with a high school education.

A multivariate analysis (Table 9) examined the relationship between independent variables and Proactive Awareness. The initial model included education and occupation, but the results showed that

not all variables had a significant impact (P < 0.05). A final model was created, which revealed that education was the only variable with a strong relationship in predicting Proactive Awareness behavior.

Table 9: Multivariate Analysis for Proactive Awareness (PA) Behavior

		B	S.E.	Wald	P-value	OR	CI 95%	
							Lower	Upper
FIRST MODEL	Education level	1.116	0.359	9.672	0.002	3.052	1.511	6.167
	Profession	0.230	0.367	0.393	0.531	1.259	0.613	2.586
FINAL MODEL	Education level	0.996	0.301	10.983	0.001	2.708	1.502	4.882

Table 10: Characteristics Comparison for Information Handling (IH) Behavior

Variable	Level of IH		OR CI 95%	P-Value
	High	Low		
	N=101	N=108		
Age			**0.771**	**0.447**
18-29	78(77.2%)	88(81.5%)	(0.393-1.510)	
30-39	23(22.8%)	20(18.5%)		
Gender			**0.690**	**0.208**
Female	30(29.7%)	41(38.0%)	(0.388-1.230)	
Male	71(70.3%)	67(62.0%)		
Education level			**2.176**	**0.007***
Higher education	70(69.3%)	55(50.9%)	(1.235-3.835)	
Highschool	31(30.7%)	53(49.1%)		
Profession			**0.633**	**0.121**
Non-medical Staff	29(28.7%)	42(38.9%)	(0.355-1.130)	
Medical staff	72(71.3%)	66(61.1%)		
Device to access HIS			**0.829**	**0.540**
Smartphone	70(69.3%)	79(73.1%)	(0.455-1.510)	
PC/Laptop	31(30.7%)	29(26.9%)		

The Chi-Square test results for Information Handling behavior (Table 10) show that age, gender, occupation, and frequently used devices are not statistically significant (P > 0.05). In contrast, the education variable has a P-value less than 0.05, indicating statistical significance. This suggests a notable difference in the proportions of education and information-handling behavior. The Odds Ratio, with a confidence interval of (1.235-3.835), reveals that healthcare workers with higher education are 2.176 times more likely to demonstrate effective information handling than those with a high school education.

Following the bivariate analysis in Table 10, a multivariate analysis (Table 11) investigates the relationship between several independent variables and information handling. The model includes gender, education, and occupation. The initial multivariate analysis shows that not all P-values for these variables are below 0.05 (P < 0.05), indicating that, collectively, they do not significantly influence information handling. Ultimately, the analysis concludes that education strongly correlates with predicting information-handling behavior.

Table 11: Multivariate Analysis for Information Handling (IH) Behavior

		B	S.E.	Wald	P Value	OR	CI 95%	
							Lower	Upper
FIRST MODEL	Gender	-0.397	0.304	1.698	0.192	0.673	0.371	1.221
	Education level	0.800	0.342	5.483	0.019	2.226	1.139	4.348
	Profession	0.024	0.357	0.004	0.947	1.024	0.509	2.060
FINAL MODEL	Education level	0.777	0.289	7.231	0.007	2.176	1.235	3.835

Table 12: Characteristics Comparison for Information Security Behavior (Overall)

Variable	Information Security Behavior		OR CI 95%	P-Value
	High	Low		
	N=104	N=105		
Age			**0.955** (0.488-1.867)	**0.892**
30-39	21(20.2%)	22(21.0%)		
18-29	83(79.8%)	83(79.0%)		
Gender			**0.752** (0.423-1.336)	**0.331**
Male	32(30.8%)	39(37.1%)		
Female	72(69.2%)	66(62.9%)		
Education Level			**2.612** (1.475-4.624)	**0.001***
Higher education	74(71.2%)	51(48.6%)		
High school	30(28.8%)	54(51.4%)		
Profession			**0.580** (0.325-1.036)	**0.064**
Non-medical staff	29(27.9%)	42(40.0%)		
Medical staff	75(72.1%)	63(60.0%)		
Device to access HIS			**0.616** (0.336-1.129)	**0.116**
Smartphone	69(66.3%)	80(76.2%)		
PC/Laptop	35(33.7%)	25(23.8%)		

The Chi-Square test results (Table 12) demonstrate that the P-values for age, gender, occupation, and frequently used devices exceed 0.05 ($P > 0.05$), indicating no statistical significance. Conversely, the education variable shows a P-value below 0.05 ($P < 0.05$), signifying statistical significance. Therefore, there is a significant relationship between education and overall information security behavior. The Odds Ratio, with a confidence interval of (1.475-4.624), indicates that healthcare workers with higher education (Diploma/Graduate) are 2.612 times more likely to exhibit better information security behavior than those with only a high school education.

Following this bivariate analysis, a multivariate analysis (Table 13) was performed to examine the impact of multiple independent variables, including education, occupation, and frequently used devices, on overall information security behavior. Initially, not all P-values were below 0.05, suggesting that these factors collectively do not significantly influence information security behavior. Ultimately, the final model confirms that only the education variable has a strong predictive relationship with overall information security behavior.

Table 13: Multivariate Analysis for Information Security Behavior (Overall)

		B	S.E.	Wald	P Value	OR	CI 95%	
							Lower	Upper
FIRST MODEL	Education level	0.915	0.351	6.799	0.009	2.497	1.255	4.967
	Profession	-0.020	0.363	0.003	0.956	0.980	0.481	1.999
	Device to access HIS	-0.098	0.349	0.079	0.779	0.907	0.458	1.797
FINAL MODEL	Education Level	0.960	0.292	10.846	0.001	2.612	1.475	4.624

4 Discussion and Implications

Despite the increasing focus on cybersecurity research within the healthcare sector, there still needs to be a significant gap in understanding non-technological factors that influence security practices (Jalali et al., 2019). Human-based components, including employee awareness, training, and behavioral tendencies, are crucial to mitigating risks associated with cyber threats. Addressing these non-technological elements is essential for developing a comprehensive cybersecurity strategy that protects

sensitive patient data and fosters a culture of security awareness throughout the organization. Further investigation into these areas is imperative to enhance resilience in evolving cyber challenges.

The results of this study indicate that among the five demographic factors analyzed for their influence on the information security behavior of healthcare workers in Indonesia, education level emerges as the most consistently impactful determinant. The research findings indicate that demographic factors influencing each dimension of information security behavior vary. The Device Protection and Password Management behavior dimension is affected by education level (higher education or high school) and profession type (medical or non-medical staff). Meanwhile, the dimensions of proactive awareness and information handling are influenced solely by education level. This suggests that education level is the most dominant factor affecting information security behavior in terms of dimension and overall. This aligns with previous research (Sari et al., 2024), which demonstrated that education influences the expected information security behavior in healthcare facilities with poor information security policies. Another study (Sari et al., 2023) also revealed that the behavior of users of health information systems, whether healthcare workers or patients, varied the most based on their education level. Despite using different samples, these three studies consistently show similar results concerning the information security behavior of healthcare workers in Indonesia.

This finding underscores the critical role that educational attainment plays in shaping the security practices and awareness of healthcare professionals in a rapidly evolving digital landscape. As healthcare systems increasingly integrate advanced technologies and digital platforms, a well-informed workforce becomes paramount (Rajamäki et al., 2018). Those with higher education levels tend to understand information security principles better, enabling them to adopt safer practices in managing sensitive patient data (Bin Md Ajis et al., 2020; Kombo et al., 2023). Furthermore, the implications of this research extend beyond immediate behavioral adjustments, suggesting that investing in educational initiatives and ongoing training programs could significantly enhance the overall security posture of healthcare institutions. By fostering a culture of continuous learning and awareness, the healthcare sector in Indonesia may not only mitigate risks associated with data breaches but also cultivate a more resilient and informed workforce capable of navigating the complexities of contemporary information security challenges. Therefore, policymakers and healthcare administrators should prioritize educational advancement as a strategic approach to strengthening information security practices within the industry.

This study provides valuable insights and contributions to the information security behavior body of knowledge. However, it does have limitations that should be considered when interpreting the findings. First, the study's cross-sectional methodology prevents causal findings, restricting the capacity to draw conclusive judgments about variable correlations over time. Furthermore, uncontrolled external factors such as environmental effects and contextual variables may have substantially impacted the study's results. Future studies should focus on designing comprehensive training programs that are specially designed to bridge the educational gaps discovered among Indonesian healthcare personnel. Investigating the impact of various instructional initiatives on employee cybersecurity practices is critical.

Further study should look at the influence of organizational culture and technology adoption rates on information security behavior. This study aims to compare the impact of demographic characteristics on information security behavior. Therefore, we do not conduct an in-depth analysis using qualitative data. We recommend that future research adopt a qualitative approach to provide more insights. Exploring the importance of ongoing professional development and its relationship to cybersecurity resilience in healthcare settings will help us better understand non-technological impacts

on security practices. Comparative research across areas and healthcare systems would yield significant insights into best practices for developing security-aware staff.

5 Conclusion

The healthcare sector needs more cybersecurity research, particularly regarding non-technological factors that impact security practices, such as employee awareness and training. This study reveals that education level is the most influential demographic factor affecting the information security behavior of healthcare workers in Indonesia, supporting previous research. A well-informed workforce is crucial as healthcare systems adopt advanced technologies, with higher education correlating to better security practices in managing sensitive data. The findings emphasize the need for enhanced educational initiatives and ongoing training to improve the security posture of healthcare institutions. Policymakers and administrators are encouraged to prioritize education as a strategic method to bolster information security within the industry.

Acknowledgements

We would like to say gratitude to Telkom University for their support to this study through Research Grant No. 113/LIT06/PPM-LIT/2024.

References

[1] Albarrak, A. I. (2011). Evaluation of Users Information Security Practices at King Saud University Hospitals. *Global Business & Management Research, 3*(1), 1–6.

[2] Alexandrou, A., & Chen, L. C. (2019). A security risk perception model for the adoption of mobile devices in the healthcare industry. *Security Journal, 32*, 410-434. https://doi.org/10.1057/s41284-019-00170-0

[3] Alumaran, S., Bella, G., & Chen, F. (2015). The role and impact of cultural dimensions on information systems security in Saudi Arabia National Health Service. *International Journal of Computer Applications, 112*(2), 21–28.

[4] Badan Siber dan Sandi Negara. (2020). *Buku Putih Keamanan Siber Sektor Kesehatan*.

[5] Badan Siber dan Sandi Negara. (2022). *Lanskap Keamanan Siber Indonesia 2022*.

[6] Bin Md Ajis, A. F., Binti Ahmad, R., Binti Osman, S., & Bin Ishak, I. (2020, April). Catalyst of Information Security in Malaysia Higher Learning Institutions. In *2020 IEEE 10th Symposium on Computer Applications & Industrial Electronics (ISCAIE)* (pp. 176-179). IEEE. https://doi.org/10.1109/ISCAIE47305.2020.9108806

[7] Boopathy, E. V., Shanmugasundaram, M., Vadivu, N. S., Karthikkumar, S., Diban, R., Hariharan, P., & Madhan, A. (2024). Lorawan based coalminers rescue and health monitoring system using Iot. *Archives for Technical Sciences, 2*(31), 213–219. https://doi.org/10.70102/afts.2024.1631.213

[8] Chairil, T. (2019). Cybersecurity for Indonesia: what needs to be done? Theconversation.com. *https://theconversation.com/cybersecurity-for-indonesia-what-needs-to-be-done-114009*

[9] Chang, H. (2015). Evaluation Framework for Telemedicine Using the Logical Framework Approach and a Fishbone Diagram. *Healthcare Informatics Research, 21*(4), 230. https://doi.org/10.4258/hir.2015.21.4.230

[10] Clementine, G., Willy, S., Thomas, P., Kaitai, L., & Duncan, S.W. (2014). Empowering Personal Health Records with Cloud Computing. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, 5*(4), 3-28.

[11] Deursen, N. Van, Buchanan, W. J., & Duff, A. (2013). Monitoring information security risks within health care. *Computers & Security*, *37*, 31–45. https://doi.org/10.1016/j.cose.2013.04.005

[12] Donalds, C., & Barclay, C. (2022). Beyond technical measures: a value-focused thinking appraisal of strategic drivers in improving information security policy compliance. *European Journal of Information Systems*, 31(1), 58–73. https://doi.org/10.1080/0960085X.2021.1978344

[13] Egelman, S., & Peer, E. (2015). Predicting privacy and security attitudes. *ACM SIGCAS computers and society*, *45*(1), 22-28. https://doi.org/10.1145/2738210.2738215

[14] Escobedo, F., Clavijo-López, R., Calle, E. A. C., Correa, S. R., García, A. G., Galarza, F. W. M., & Flores-Tananta, C. A. (2024). Effect of Health Education on Environmental Pollution as a Primary Factor in Sustainable Development. *Natural and Engineering Sciences*, *9*(2), 460-471. http://doi.org/10.28978/nesciences.1574456

[15] Fernández-alemán, J. L., Sánchez-henarejos, A., Toval, A., Sánchez-garcía, A. B., Hernández-hernández, I., & Fernandez-luque, L. (2015). Analysis of health professional security behaviors in a real clinical setting : An empirical study. *International Journal of Medical Informatics*, *84*, 454–467. https://doi.org/10.1016/j.ijmedinf.2015.01.010

[16] Hadlington, L. (2017). Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviors. *Heliyon*, *3*(7), e00346. https://doi.org/10.1016/j.heliyon.2017.e00346

[17] Ifinedo, P., & Akinnuwesi, B. A. (2014, October). Employees' non-malicious, counterproductive computer security behaviors (CCSB) in Nigeria and Canada: an empirical and comparative analysis. In *2014 IEEE 6th International Conference on Adaptive Science & Technology (ICAST)* (pp. 1-7). IEEE. https://doi.org/10.1109/ICASTECH.2014.7068109

[18] Jalali, M. S., Razak, S., Gordon, W., Perakslis, E., & Madnick, S. (2019). Health care and cybersecurity: bibliometric analysis of the literature. *Journal of medical Internet research*, *21*(2), e12644. https://doi.org/10.2196/12644

[19] Karimov, N., & Sattorova, Z. (2024). A Systematic Review and Bibliometric Analysis of Emerging Technologies for Sustainable Healthcare Management Policies. *Global Perspectives in Management*, *2*(2), 31-40.

[20] Kessler, S. R., Pindek, S., Kleinman, G., Andel, S. A., & Spector, P. E. (2020). Information security climate and the assessment of information security risk among healthcare employees. *Health Informatics Journal*, *26*(1), 461–473. https://doi.org/10.1177/1460458219832048

[21] Kombo, F. S., Mwakalinga, P. G., Kumbo, L. I., Edward, L. M., & Bhalalusesa, N. P. (2023). Assessment of Higher Education Information Security Risk Management Practices in Tanzania. *East African Journal of Education and Social Sciences*, *4*(3), 229–239. https://doi.org/10.46606/eajess2023v04i03.0294

[22] Krishnan, H., Santhosh, Vijay, & Yasmin, S. (2022). Blockchain for Health Data Management. *International Academic Journal of Science and Engineering*, *9*(2), 23–27. https://doi.org/10.9756/IAJSE/V9I2/IAJSE0910

[23] Mishra, S., Caputo, D. J., Leone, G. J., Kohun, F. G., & Draus, P. J. (2014). The Role of Awareness and Communications in Information Security Management: A Health Care Information Systems Perspective. *International Journal of Management & Information Systems*, *18*(2), 139–148. https://doi.org/10.19030/ijmis.v18i2.8495

[24] Nifakos, S., Chandramouli, K., Nikolaou, C. K., Papachristou, P., Koch, S., Panaousis, E., & Bonacina, S. (2021). Influence of Human Factors on Cyber Security within Healthcare Organisations: A Systematic Review. *Sensors*, *21*(15), 5119. https://doi.org/10.3390/s21155119

[25] Nunes, P., Antunes, M., & Silva, C. (2021). Evaluating cybersecurity attitudes and behaviors in Portuguese healthcare institutions. *Procedia Computer Science*, *181*, 173–181. https://doi.org/10.1016/j.procs.2021.01.118
[26] Osei-Bryson, K. M., Brown, I., & Meso, P. (2022). Advancing the development of contextually relevant ICT4D theories-from explanation to design. *European journal of information systems*, *31*(1), 1-6. https://doi.org/10.1080/0960085X.2022.1994119
[27] Parsons, K., Calic, D., Pattinson, M., Butavicius, M., McCormac, A., & Zwaans, T. (2017). The Human Aspects of Information Security Questionnaire (HAIS-Q): Two further validation studies. *Computers and Security*, *66*, 40–51. https://doi.org/10.1016/j.cose.2017.01.004
[28] Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2014). Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q). *Computers and Security*, *42*, 165–176. https://doi.org/10.1016/j.cose.2013.12.003
[29] Rajamäki, J., Nevmerzhitskaya, J., & Virág, C. (2018). Cybersecurity education and training in hospitals: Proactive resilience educational framework (Prosilience EF). 2*018 IEEE Global Engineering Education Conference (EDUCON)*, 2042–2046. https://doi.org/10.1109/EDUCON.2018.8363488
[30] Sari, P. K., Handayani, P. W., & Hidayanto, A. N. (2023). Demographic Comparison of Information Security Behavior Toward Health Information System Protection: Survey Study. *JMIR Formative Research*, *7*, e49439. https://doi.org/10.2196/49439
[31] 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. *Pacific Asia Conference on Information Systems (PACIS)*. https://aisel.aisnet.org/pacis2024
[32] Surendar, A. (2024). Internet of Medical Things (IoMT): Challenges and Innovations in Embedded System Design. *SCCTS Journal of Embedded Systems Design and Applications*, *1*(1), 33-36.
[33] Vanan, J. T., Manalan, J., Soundrarajan, D. J., & Raja, T. (2019). Awareness and Utilization of Electronic Resources among Junior Research Fellows with Special Reference to Christian Medical College & Hospital, Vellore, Tamil Nadu. *Indian Journal of Information Sources and Services*, *9*(S1), 32-36. https://doi.org/10.51983/ijiss.2019.9.S1.569
[34] Verizon. (2019). 2019 Verizon data breach investigation report. https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf

Authors Biography

Puspita Kencana Sari is an assistant professor at the Faculty of Economics and Business, Telkom University, where she also heads the Center of Excellence in Economics of Advanced Digital Technology. She holds a doctorate in Computer Science from the Universitas Indonesia, with research interests in information security management, IS user behavior, e-commerce, and e-health.

Nurvita Trianasari is an assistant professor at the Faculty of Economics and Business at Telkom University, where she also serves as the Head of the Business Digital Study Program. She earned her doctorate in Statistics and data science from the Faculty of Science and Math at the Institut Pertanian Bogor and focuses her research on applied statistics.

Adhi Prasetio is an associate professor at the Faculty of Economics and Business, Telkom University. He earned his doctorate in Management from Universitas Pendidikan Indonesia and focuses his research on e-commerce, marketing management, and social media marketing.