Interdisciplinary Journal of Information, Knowledge, and Management

An Official Publication of the Informing Science Institute InformingScience.org

IJIKM.org

Volume 18, 2023

How Information Security Management Systems Influence the Healthcare Professionals' Security Behavior in a Public Hospital in Indonesia

Puspita Kencana Sari*	University of Indonesia, Depok, Indonesia; Telkom University, Bandung, Indonesia	puspita.kencana91@ui.ac.id
Putu Wuri Handayani	University of Indonesia, Depok, Indonesia	putu.wuri@cs.ui.ac.id
Achmad Nizar Hidayanto	University of Indonesia, Depok, Indonesia	nizar@cs.ui.ac.id
Pribadi Wiranda Busro	National Cardiovascular Center Harapan Kita, Jakarta, Indonesia	pribadiwb@yahoo.com

* Corresponding author

Abstract

Aim/Purpose	This study analyzes health professionals' information security behavior (ISB) as health information system (HIS) users concerning associated information security controls and risks established in a public hospital. This work measures ISB using a complete measuring scale and explains the relevant influential factors from the perspectives of Protection Motivation Theory (PMT) and General Deterrence Theory (GDT)
Background	Internal users are the primary source of security concerns in hospitals, with malware and social engineering becoming common attack vectors in the health industry. This study focuses on HIS user behavior in developing countries with limited information security policies and resources.
Methodology	The research was carried out in three stages. First, a semi-structured interview was conducted with three hospital administrators in charge of HIS implementation to investigate information security controls and threats. Second, a survey of 144 HIS users to determine ISB based on hospital security risk. Third, a

Accepting Editor Dimitar Grozdanov Christozov | Received: May 22 2023 | Revised: August 23, August 29, 2023 | Accepted: August 30, 2023.

Cite as: Sari, P. K., Handayani, P. W., Nizar, A., & Busro, P. W. (2023). How information security management systems influence the healthcare professionals' security behavior in a public hospital in Indonesia. *Interdisciplinary Journal of Information, Knowledge, and Management*, *18,* 583-607. https://doi.org/10.28945/5185

	semi-structured interview was conducted with 11 HIS users to discuss the elements influencing behavior and current information security implementation.
Contribution	This study contributes to ISB practices in hospitals. It discusses how HIS managers could build information security programs to enhance health professionals' behavior by considering PMT and GDT elements.
Findings	According to the findings of this study, the hospital has implemented particular information security management system (ISMS) controls based on international standards, but there is still room for improvement. Insiders are the most prevalent information security dangers discovered, with certain working practices requiring HIS users to disclose passwords with others. The top three most common ISBs HIS users practice include appropriately disposing of printouts, validating link sources, and using a password to unlock the device. Meanwhile, the top three least commonly seen ISBs include transferring sensitive information online, leaving a password in an unsupervised area, and revealing sensitive information via social media.
Recommendations for Practitioners	Hospital managers should create work practices that align with information security requirements. HIS managers should provide incentives to improve workers' perceptions of the benefit of robust information security measures.
Recommendations for Researchers	This study suggests more research into the components that influence ISB utilizing diverse theoretical foundations such as Regulatory Focus Theory to compare preventive and promotion motivation to enhance ISB.
Impact on Society	This study can potentially improve information security in the healthcare industry, which has substantial risks to human life but still lags behind other vital sector implementations.
Future Research	Future research could look into the best content and format for an information security education and training program to promote the behaviors of healthcare professionals that need to be improved based on this ISB measurement and other influential factors.

Keywords	information security behavior, hospital, health information system, protection motivation, deterrence

INTRODUCTION

Information systems can assist in delivering more effective and efficient health care, but they can also raise information security risks, such as Ransomware threats that target hospitals in several nations (Interpol, 2020; Jercich, 2021). Attacks on hospitals in the United States, Australia, and Germany (Tidy, 2020; Tonkin, 2021) interrupted healthcare operations and endangered patients' lives. According to the Enterprise Strategy Group Study (Oltsik, 2020), cyberattacks have increased during the pandemic due to employees lacking proper expertise or security training for work from home, such as dealing with internet scams and phishing emails.

According to previous research (Bakkar & Alazab, 2019; Fatima & Colomo-Palacios, 2018; Samy et al., 2010), most security concerns in hospitals are triggered by internal staff. Accidental disclosure, insider curiosity, data breaches by insiders, data breaches by outsiders with physical tampering, and meddling with network systems are all security hazards to healthcare businesses (Fernández-Alemán et al., 2015). Three of the five types are considered insider threats because they originate within companies. Healthcare security vulnerabilities are caused by networked and accessible medical devices, old systems no longer supported, and a lack of interest in information security (Coventry & Branley,

2018). Implementing a health information system (HIS) to keep patient data in an electronic system presents problems relating to data quality and dependability, raising potential risks to patient safety (Layman, 2008; Ozair et al., 2015).

The health industry is one of the top five industries in Indonesia that may experience the most cybersecurity attacks in 2022, with data breaches, website defacements, and ransomware being the most common events (Badan Siber dan Sandi Negara, 2022). In 2017, two big public hospitals in Indonesia were targeted by the WannyCry Ransomware, resulting in health professionals being unable to access pertinent information, preventing many surgical operations from being performed, and putting patients' lives in danger (Kertopati, 2017). Although the number of hospitals attacked was not huge, attacks on big-scale hospitals might have a significant impact. In 2020, 230,000 COVID-19 patients' data, including personal information and medical examination results, reportedly from a hospital in Indonesia, were sold on the dark web (CNN-Indonesia, 2020; Kumparan, 2020). The most frequent attack vector for these occurrences is a compromised account by malware thieves or social engineering by end-users who click on a malicious link or email attachment designed to execute malicious code on the victim's workstation (Badan Siber dan Sandi Negara, 2022). Threat actors also exploit hacked websites to infect end-user devices when they download applications from the website. Threat actors use genuinely compromised accounts rather than malware, which the security perimeter is more likely to detect. The threat to security is projected to increase in 2023 (Badan Siber dan Sandi Negara, 2022). Meanwhile, Indonesia still needs more healthcare facilities with adequate information security infrastructure (Burhan, 2020). Therefore, managing end-user security behavior is critical for health organizations to anticipate this threat vector, thus increasing patient safety.

According to the Healthcare Information and Management Systems Society (HIMSS) survey, the standard from the International Organization for Standardization (ISO) is one of the most often employed information security standards in healthcare organizations (Calyptix, 2018). ISO/IEC 27799:2016 is part of the ISO/IEC 27000 series focusing on information security in the healthcare industry. The Indonesian government has also recognized ISO/IEC 27000 as a reference for general organizations' Information Security Management System (ISMS) implementation. ISO/IEC 27799:2016 has been adopted, becoming the national standard SNI 27799:2017, but has yet to be reduced to a formal rule for healthcare facilities (PERSI, 2022). ISO/IEC 27799:2016 provides security controls, security threats, action plans, and self-assessment guidelines for implementing ISMS in healthcare organizations.

Studies on how humans affect information security-related incidents in hospitals have been limited (Ahouanmenou et al., 2022). Advanced information systems necessitate knowledgeable workers to avoid security breaches while adhering to established ISMS rules; thus, health professionals' information security knowledge and behavior must be quantified (Nunes et al., 2021). This study investigates HIS users' information security behavior (ISB) using a comprehensive measuring scale tailored to healthcare information security risks. The Human Aspects of Information Security Questionnaire (HAIS-Q) (Parsons et al., 2014, 2017), Security Behavior Intentions Scale (SEBIS) (Egelman & Peer, 2015), Risky Cybersecurity Behavior Scale (RSCB) (Hadlington, 2017), and Counterproductive Computer Security Behaviors (CCSB) (Ifinedo & Akinnuwesi, 2014) are several frameworks for measuring ISB from previous literature. This study uses security behavior indicators from frameworks related to hospital information security concerns. After assessing their security behavior, it is critical to identify antecedent variables for HIS users' security behavior. Existing research on the relationship between information security behavior assessment and influencing variables still needs to be completed.

Previous researchers have discovered traits that affect non-compliance behavior in hospitals (Liginlal et al., 2012) and the disclosure of patient information to unauthorized individuals (Park et al., 2017, 2018). Other researchers have looked at a variety of factors that influence compliance behavior with organizational security policies (Foth et al., 2012; Pathania & Rasool, 2019; Sher et al., 2017), information security regulations (Brady, 2011; Foth, 2016; Johnston & Warkentin, 2008), and information

security standards (Alexandrou & Chen, 2019; Fernández-Alemán et al., 2015). According to the outcomes of a systematic literature review (Sari et al., 2022), previous studies in information security behavior in the healthcare context typically employ theoretical foundations such as Protection Motivation Theory (PMT) and General Deterrence Theory (GDT) in conjunction with other theories such as Theory of Planned Behavior (TPB), Theory of Acceptance Model (TAM), Social Cognitive Theory (SCT), Rational Choice Theory (RCT), and many others. However, these theories have been used to investigate healthcare staff's security behavior in developed countries. Prior studies (Ndibwile & Luhanga, 2018; Sawaya et al., 2017) indicated that security behavior differs across developing and developed nations due to motivation and decision-making. As a result, validating the idea in developing nations such as Indonesia is still required.

This research objective is to examine the information security behaviors of HIS users, compliance, and non-compliance in a public hospital in Indonesia. This study proposes four research questions (RQ) to address the problems:

- RQ1. What are existing information security controls established in the hospital?
- RQ2. What are information security threats to health information system (HIS) usage in the hospital?
- RQ3. How is the information security behavior of HIS end-users?
- RQ4. What factors can influence the information security behavior of HIS end-users in accordance with the PMT and GDT framework?

This study makes both a practical and theoretical contribution. In terms of practical contribution, the results provide recommendations for information security managers in the hospital by considering security controls, threats, typical security behavior of users, and factors that impact them. This study contributes theoretically to the knowledge of information security behavior, particularly in hospitals in developing countries such as Indonesia.

This paper is divided into the five sections. The first section reviews the related literature background adopted in this study. The second section then describes the study design, including the sampling process and data analysis approach. The results and extensive discussion are presented in the third and fourth sections. The final part reviews the conclusion, study implications, and future research.

LITERATURE REVIEW

ISO 27799:2016 provides guidelines and best practices for implementing and managing information security within the healthcare industry. It addresses the unique challenges and risks of protecting sensitive patient data in health informatics systems. ISO 27799 has 14 security control clauses that healthcare organizations can adopt to ensure patient information confidentiality, integrity, and availability (International Organization for Standardization, 2016). The resume for control clauses can be seen in Table 1. By implementing these controls, healthcare organizations can enhance their overall information security posture and mitigate potential threats to patient data. It also provides some examples of threats to health information assets, such as masquerades by insiders, service providers, or outsiders; unauthorized use of a health information application; introduction of disruptive software; misuse of system resources; communication infiltration and interception; repudiation; connection failure; technical failure; user error; theft by insiders or outsiders; and others. These threats can lead to various consequences, including unauthorized access to patient data, compromised privacy, and confidentiality, disruption of healthcare services, financial losses, and damage to the reputation of healthcare organizations. Implementing robust security measures and regular monitoring can help prevent these threats and ensure the integrity and availability of health information assets.

Table 1. Security control clauses in ISO 27799:2016

CONTROL CLAUSES	SCOPE OF CONTROL
Information security policy	Establishment and review of information security policies as a form of management direction
Organization of information security	An organizational structure that describes the duties and responsibilities for implementing information security, including relationships with related parties and policies on the use of mobile devices and teleworking
Human resources security	Management of human resources so that they can support the protection of information security in the organization, including the recruitment process, during the working period, employee turnover, and termination
Asset management	Management of assets used in the collection, processing, and storage of information, including assigning responsibilities for assets, classifying information, and handling media when transferred or destroyed
Access control	Management of user access rights to information systems and networks according to their roles and responsibilities, including access rights policies, standard operating procedures, review and adjustment of access rights
Cryptography	Controlling the application of cryptography technology in information systems, including policies on the use of cryptography and key management
Physical and environmental security	Determination of organizational safe areas based on the physical perimeter, including rooms, facilities, and certain areas to secure equipment and supporting devices such as user desktops
Operation security	Establishment of security controls for the organization's operational processes, including establishing operational procedures and responsibilities, protection from malware, backups, operational software management, technical vulnerability management, and information system audit controls
Communication security	Security controls on security processes, such as network security management and information transfer operations, are implemented through confidentiality agreements with connected parties.
System acquisition, development, and maintenance	Security management is acquiring, developing, and maintaining systems, including information system security requirements, development policies, change procedures, and data protection for system trials.
Supplier relationships	Security control related to cooperation with third parties, including policies, agreements, supply chain information technology, to managing changes to cooperation.
Information security incident management	Information security incident management, including incident reporting; reporting of security holes; incident assessment; incident response; and collection of supporting data
Information security aspects of business continuity management	Application of information security in business continuity, including planning, implementation, verification, review, and evaluation of sustainability and availability of information processing facilities.
Compliance	Control of compliance with legal requirements, policies, and standards, and technical compliance through regular information security reviews.

HAIS-Q and SEBIS measure more security behavior in favor of information security protection. In contrast, the RSCB and CCSB focus on risky security behavior leading to information security incidents. Previous studies in the health context mainly employed HAIS-Q (Aljedaani et al., 2020; Fauzi et al., 2021; Pollini et al., 2022; Schmidt et al., 2021), or it was coupled with SEBIS (Fauzi et al., 2021) and the RSCB (Nunes et al., 2021). Most studies use health workers as subjects (Fauzi et al., 2021; Nunes et al., 2021; Pollini et al., 2022; Schmidt et al., 2021). The most dangerous behavior of health personnel is viewing external websites using hospital computers (Aljedaani et al., 2020). SEBIS was developed on best practices for Internet security and sensitive information protection. SEBIS comprises 16 indicators organized into four dimensions: device security, password generation, proactive awareness, and updating behavior. HAIS-Q utilizes a knowledge-attitude-behavior model established in response to empirical investigations on human errors. HAIS-Q contains 63 indicators organized into three dimensions, each with seven focused areas: password management, email use, Internet use, social networking site use, incident reporting, mobile computing, and information handling. This study mainly looks at indicators from the behavior dimension. CCSB is based on social cognitive theory and includes 12 indicators grouped into three dimensions: careless use of IS resources, procrastination on needed IS actions, and improper use of IS resources. The RSCB extends from the SEBIS measuring scale by including four additional indicators and examining behavior that might contribute to harmful cybersecurity practices.

According to PMT, protection motivation derives from a cognitive appraisal of the threat (refer to threat appraisal) combined with an understanding that the prescribed countermeasure reaction can effectively prevent unpleasant incidents from occurring (refer to coping appraisal) (Rogers, 1975). Threat appraisal includes perceived severity and susceptibility, and coping appraisal includes response efficacy, self-efficacy, and cost (Norman et al., 2005). In the context of information security behavior in the Health Facilities environment, perceived susceptibility refers to HIS users' beliefs about the possibility of receiving a security threat. In contrast, perceived severity refers to the user's beliefs about the potentially harmful effects of the HIS (Alexandrou & Chen, 2019). Several studies have utilized the term perceived benefit to describe response effectiveness, which refers to HIS users' opinions that there are possible advantages to preserving information assets (Sher et al., 2017). The same study used perceived barriers rather than reaction costs to explain user perceptions of information security's physical and psychological costs. The user's view impacts his or her protection motive, motivating the user to engage in information security behavior. Protection motivation might be low if the user believes the security threat is not too severe and will not affect him. The hurdles to protection are perceived to be more significant than the advantages. Users are more prone to participate in risky security behavior, threatening information security.

The efficiency of various security solutions is assessed using the model's four countermeasures: deterrent, prevention, detection, and remedies (Dreyfuss & Giat, 2016). As a result, as the final stage in this study, we use GDT to assess the deterrent factors impacting information security behavior. GDT (Straub & Welke, 1998) derived from the field of criminology and states that the prevention of criminal acts can be accomplished by informing those who have the potential to commit such acts about the punishment to be received (severity of penalty) and the certainty of supervision of the violation (certainty of detection). Straub and Welke (1998) added security countermeasures such as security policies, awareness programs, education and training (SETA), and computer monitoring to the field of information systems, specifically related to information security, as factors that affect the desire to comply (compliance intention) through two variables from Deterrence Theory (D'Arcy et al., 2009). When users are aware that the penalties for non-compliance in data protection are severe and that their activities using CIS are being monitored, they are more likely to reduce unwanted behavior; conversely, if they believe the penalties are not severe or that there is no apparent supervision (Foth, 2016).

The constructs in PMT and GDT used in this study are described in Table 2.

Table 2. Constructs in PMT and GDT

FOUNDATIONAL THEORY	CONSTRUCTS	DESCRIPTION
General Deterrence Theory (GDT)	Management support	Top management or organizational commitment to information security is critical for the overall effectiveness of the hospital's information security implementation.
	Security monitoring	Specific data protection activities or processes must be enforced throughout the hospital.
	Regulatory awareness	The possibility of violating security and privacy norms when utilizing HIS.
Protection Motivation Theory (PMT)	Perceived benefit	Subjective evaluation of the advantages or positive outcomes an individual believes they will experience due to information security measures.
	Perceived barrier	Subjective evaluation of difficulty or cost of security practices, including money, time, or effort, that can deter individuals from implementing necessary security measures.
	Perceived severity	Subjective evaluation of the potential harm caused by the security incident or threat.
	Perceived susceptibility	Perceived susceptibility is a perception of the possibility of exposure to dangerous security threats and the likelihood of experiencing negative consequences.

METHODOLOGY

This study uses a case study from the National Cardiovascular Center Harapan Kita (RSPJNHK), a specialized public hospital in Indonesia that serves as a national referral center for heart and circulatory disease treatment (Ethical approval number: LB.02.01/VI/453/KEP 036/2020). RSJPNHK has established an information technology (IT) implementation policy since 2017. The IT Department developed its own HIS, including Electronic Medical Records (EMR), e-prescription, patient registration system, and many back-end applications to support its services. RSJPNHK is one of the hospitals that received a positive evaluation for information security from the National Cyber and Crypto Agency (BSSN). The data has been collected only from one state-owned hospital in Indonesia for several reasons. Firstly, this hospital was chosen as it is one of the country's most extensive and well-equipped healthcare facilities, making it a representative sample for studying healthcare trends and patterns. Focusing on a single hospital also allows for a more in-depth analysis of the specific healthcare system and its performance.

We conducted three phases to address the research questions. The first phase uses the qualitative study to explore hospital information security threats and controls to address RQ1 and RQ2. We adopt ISO 27799:2016 control clauses and security threats. We collect the data using an interview with the Head of the IT Department, the units responsible for HIS provider, and the Head of the Medical Record Department, responsible for the hospital's medical records and health information management. Data from interviews were processed using a thematic coding analysis technique that separated into two stages: first-cycle and second-cycle (Saldaña, 2013). The coding analysis begins

with generating transcripts of each interviewee and then entering them into qualitative data processing tools such as NVivo 12. The first-cycle coding approach is used for initial data coding. In contrast, the second-cycle coding method is used for categorizing, prioritizing, integrating, synthesizing, abstracting, creating ideas, and building theories based on the findings of the first-cycle coding (Saldaña, 2013). In this phase, the initial codes are taken from control clauses and security threats in ISO 27799:2016. The codes are mapped into implemented information security protection and security risks in the hospital, as mentioned by interviewees. The analysis results are utilized to develop information security behavior indicators, which will be reviewed in the following step.

The second phase is a quantitative study to measure security behavior based on the qualitative results to address RQ3. The four prior ISB frameworks are adjusted and used as research instruments in this study. As an initial step, we refer to the SeBIS framework, which has more on examining information security behavior than HAIS-Q, which assesses information security awareness, even though HAIS-Q is more often used for research in the health sector. This questionnaire includes demographic items and the 5-point Likert scale for security behavior items. We collect the data through online and offline surveys using questionnaires to medical and non-medical staff in the hospital, including temporary staff. Since the number of populations might change during this study, we used a non-probability sampling method with a minimum target sample of 100 (Zikmund et al., 2010). The method used is descriptive statistics using IBM SPSS and Microsoft Excel software to visualize the information security behavior of HIS users. We conducted reliability tests using IBM SPSS software for all survey items with Cronbach alpha. If the value is above 0.7, the instrument is reliable. We also conducted a validity test with Pearson correlation. All items that have Sig. < 0.05 means valid and can be used for further analysis. For descriptive analysis, we calculate the mean value for each item. The higher mean value indicates better ISB, which means more frequently adopting desirable security behavior and less frequently adopting undesirable security behavior.

The third phase uses a qualitative study to explain the influence factors of information security behavior from the quantitative results in the second phase and the relation to established security controls from the qualitative results in the first phase. This phase addresses RQ3. We collected the data using a semi-structured interview with a target of 10% of respondents from the quantitative phase. We chose individuals from each profession, gender, age, and educational level to elicit explanations from all categories of respondents. Thematic coding analysis approaches were used to process interview transcripts using NVivo software, as in the first phase, to answer RQ1 and RQ2. The constructs in the theoretical frameworks of PMT and GDT (Table 1) are used to generate initial codes in the first-cycle coding. It is likely that elements other than the constructs of PMT and GDT would be gathered from the interviewees' explanations and generate new code. Figure 1 describes the research flow to address the research questions using three study phases.

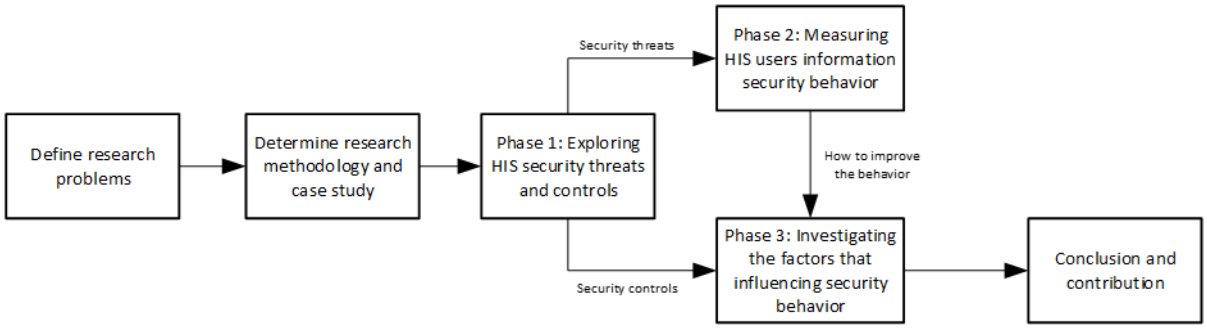

Figure 1. Research flowchart

DATA ANALYSIS RESULT

PHASE 1. QUALITATIVE STUDY: EXPLORING INFORMATION SECURITY THREATS AND CONTROLS

We interviewed the Head of the IT Department (N1), the Head of the Medical Record Department (N2), and the Head of the System Maintenance and Security Sub-unit (N3). Due to the resource individuals' hectic schedules, the interview was done three times. We investigated security measures established in hospitals using the self-assessment guideline in Appendix ISO 27799:2016. In the initial coding step, we linked the interview transcript with the security controls clauses (Table 1). We also include an explanation for each security control deployed in the hospital. Table 3 displays each security control clause's interview transcript coding results.

Table 3. Information security control in the hospital mapped into ISO 27799:2016

SECURITY CONTROL (ISO 27799:2016)	INFORMATION SECURITY CONTROLS IN THE HOSPITAL	
	DESCRIPTION	INTERVIEWEE'S NOTE
Information security policy	The hospital has established HIS implementation policy, including information security management but has yet to explicitly refer to information security standards such as ISO/IEC 27000. It has established standard operational procedures (SOP) for access control, patient privacy and confidentiality, network, physical security, and others.	"*.. There is a policy from the hospital's Director about information system usage (Guideline for Data and Information Technology Management) that consists of information security although not specifically adopting ISO 27000.*" [N1]
Information security organization	System Maintenance and Security Sub-unit in the IT Department (SIRS) is also responsible for hospital information security, especially database and network security.	"*The main function of the information security (unit) is to manage the data center, both the server and the database systems. Then the security system and network system…*" [N1]
Human resource security	There needs to be specific information security training to improve end-user security awareness. Information security education is usually given through circular letters or training for new employees.	*"(We) make a circular letter to the unit and every new user (via) email. There is no application (training) yet …*" [N1]
Asset management	Since the hospital is a public organization, all hardware should be reported to the Ministry of Finance and have an asset registry number. There is no information assets classification based on criticality.	"*Assets in the form of hardware are recorded since they become hospital and state assets ... As for the data, it is not specifically separated. There is no grouping based on its criticality.*" [N1]
Access control	User access rights are regulated in the Director's regulations. The hospital has defined employees' access rights at the beginning of the working period and when they move to another work unit.	*"The Director's Circular Letter regarding Information System Access Rights contains details regarding password settings, password requirements, then sanctions for violations of the use of access rights.*" [N1]
Physical and environmental security	The hospital established safe areas for the data center room, such as using fingerprints for authorized staff, fire alarms, and smoke detectors. There is no standard physical security. Every department is responsible for its assets.	*"… the server room uses fingerprints that not everyone can enter (into the room) ... We install alarms, fire extinguishers, sensors for smoke, and other controls. In the user room, there is no (security protection) because each unit manages the physical assets."* [N1]

SECURITY CONTROL (ISO 27799:2016)	INFORMATION SECURITY CONTROLS IN THE HOSPITAL	
	DESCRIPTION	INTERVIEWEE'S NOTE
Communication security	The hospital uses firewalls and antiviruses to protect hardware and network devices in servers and workstations. There are no specific information exchange arrangements.	"*From the server side, we install security devices; from the PC user side, we install antivirus. If that (information sharing) has not been specifically regulated.*" [N1]
Supplier (third party) relationship	Hospitals use third-party services such as Internet providers, data center maintenance, and medical device maintenance. There are no standard provisions on information security regarding access rights to systems and data.	*"Usually, there is a contract regarding what can be accessed. There are no standard provisions, but usually, the access rights are according to the contract period."* [N1]
Incident management	The hospital has established procedures for incident reporting through the Helpdesk using a specific phone line. Incidents reported to the Helpdesk will only be logged if follow-up is required, such as device replacement. Incident escalation is carried out in stages to the technical team or related vendors but has never been reported to the government's incident response team (BSSN).	*"The user already knows if, for example, there is an incident, a virus, or something, report it to the help desk. The help desk officer guides if the nature (incident) can be guided by telephone. If not, escalate to the technical team. Later, if the technical team cannot (handle it) report it to the top again. However, for security, it has never been escalated (to BSSN). Incidents that are recorded are usually tangible ..."* [N1]
Compliance	The hospital has yet to conduct a specific information security audit. Regular assessment for compliance only focuses on users' access control. The Department of Medical Records conducts data integrity audits for electronic medical records regularly to review the completeness and correctness of the data.	"*It is called a closed medical record review. Later we will review everything from the anamnesis, physical examination, and primary and secondary diagnoses. Is it true or not the contents of the resume, whether connected to the diagnosis, medication, and length of stay.*" [N2]

In this interview session, we also discuss information security threats that have occurred or may occur at the hospital. According to the history of information security breaches in hospitals, the most typical vulnerability is insider masquerade, in which users exchange their credentials. One reason for this incidence is the requirement to validate medications delivered by other health personnel while the user is also delivering services. It prompts users to share passwords to carry out the verification procedure so that patients' service is not delayed. Table 4 maps information security threats from internal sources with ISO/IEC 27799:2016 threat categories.

Table 4. Internal security threats

TYPE OF SECURITY THREATS (ISO 27799:2016)	RELATED SECURITY RISKS IN THE HOSPITAL	INTERVIEWEE'S NOTE
Masquerade by insiders	User shares their accounts and password to be used by other staff.	*"Sometimes the password, for various reasons, is shared with people he trusts.*" [N1]
User error	The user must correct an error when entering data into the HIS, resulting in inaccurate or incomplete data.	*"Even when the required field is used, EMR data is not filled out.*" [N2]
Unauthorized use of health information application	The user modifies data that should not be on the EMR system.	*"Changes to patient medical resume data by an authorized user (resident on duty at the hospital).*" [N1]

TYPE OF SECURITY THREATS (ISO 27799:2016)	RELATED SECURITY RISKS IN THE HOSPITAL	INTERVIEWEE'S NOTE
Misuse of system resources	People use computer networks and devices to browse websites that are unrelated to their jobs.	*"Employees utilized IT resources (PCs and the Internet) for personal benefit prior to the firewall filter's implementation."* [N3]
Maintenance error	The system was interrupted during maintenance due to network or device configuration problems.	*"The system's (access to) performance is slowed due to network maintenance."* [N3]
Application software failure	The system needs to meet stakeholders' expectations, which may be due to a shortage of IT employees to build applications.	*"The high risk in the IT Unit comprises operational risk, including timely fulfillment of application requests owing to a shortage of human resources..."* [N1]

The informant also identified some information security problems at the hospital caused by non-HIS users, such as masquerade by outsiders, technical failure, and disruptive software. Table 5 depicts the mapping of external security threats in ISO/IEC 27799:2016 by threat category. Threats of outsiders stealing devices have never occurred and have not been expressly acknowledged by interviewees. However, there is no physical security control in the user's room, whereas the hospital is an open area freely accessible to outsiders. It raises the possibility of stealing users' mobile devices, commonly used to access HIS.

Table 5. External security threats

TYPE OF SECURITY THREATS (ISO 27799:2016)	RELATED SECURITY RISKS IN THE HOSPITAL	INTERVIEWEE'S NOTE
Masquerade by outsider	Unauthorized individuals (such as patients) have accessed and recorded information on the EMR.	*"A photograph showing the patient's EMR system's screen display (user interface)."* [N1]
Technical failure	Interference with the power supply causes a server disruption.	*"... (occurs) an electrical malfunction that renders the system inoperable."* [N2]
Introduction of disruptive software	Cyberattacks that can harm data, such as ransomware, malware, and viruses	*"Most malware infections occur on a workstation acquired from the Internet without the user's knowledge. Some are affected since the flash disk is being utilized."* [N1]
Theft by outsiders	No physical protection exists in the user's work area (such as a nurse station), raising the danger of mobile device theft and confidential documents.	*"In the user room, there is no (security protection) because each unit manages the physical assets …"* [N1]

Formulating information security behavior indicators

After determining security threats in the hospital, we mapped them to ISB measurement scales, consisting of SEBIS, HAIS-Q, RSCB, and CCSB. Indicators in two or more frameworks are the primary candidates for use as indicators in this study. If these indicators were consistent with the threats and risks in the hospital, they were included in the survey's items. We also added some indicators that appear in only one framework if they are related to information security risks in the hospital. Table 6 shows 28 research indicators for the second phase study. The ISB indicators are divided into four focus areas adopting the SEBIS framework, namely: Device protection (codes 1.1 to 1.6), Password management (2.1 to 2.6); Proactive awareness (3.1 to 3.10); and Information handling (4.1 to 4.6). We measure desirable and undesirable security behavior for each focus area equally.

Table 6. Research variables for the quantitative phase

CODE	ISB INDICATORS	SECURITY BEHAVIOR FRAMEWORK	INFORMATION SECURITY THREATS IN HOSPITAL
1.1	Locking workstation when idle	SEBIS, HAISQ	Unauthorized use of health information application
1.2	Using passwords to unlock devices	SEBIS	Unauthorized use of health information application
1.3	Physically securing mobile devices	HAISQ, CCSB	Theft by outsiders
1.4	Not logging out of secure systems after use*	CCSB	Unauthorized use of health information application
1.5	Not checking for software (antivirus, operation system) updates*	SEBIS, RSCB, CCSB	Introduction of disruptive software
1.6	Disabling the antivirus to download from websites*	RSCB	Introduction of disruptive software
2.1	Using strong password	SEBIS, HAISQ, RSCB, CCSB	Masquerade by outsiders
2.2	Using a different password for different account	SEBIS, HAISQ, RSCB	Masquerade by outsiders
2.3	Updating work-related passwords regularly	CCSB	Masquerade by outsiders
2.4	Pasting or sticking computer passwords in a visible place*	CCSB	Masquerade by outsiders & insiders
2.5	Password sharing*	HAISQ, RSCB, CCSB	Masquerade by insiders
2.6	Never change the default password*	SEBIS, HAISQ	Masquerade by insiders
3.1	Verifying website before submitting information online	SEBIS, HAISQ, RSCB	Masquerade by outsiders
3.2	Verifying the source before clicking on links	SEBIS, HAISQ, RSCB	Introduction of disruptive software
3.3	Opening attachments in emails from a trusted sender	HAISQ	Introduction of disruptive software
3.4	Social media privacy setting	HAISQ	Masquerade by outsiders
3.5	Accessing dubious or non-related websites*	SEBIS, HAISQ, CCSB	Introduction of disruptive software
3.6	Downloading files (antivirus, digital media, data, and other material) from unknown sources*	HAISQ, RSCB, CCSB	Introduction of disruptive software
3.7	Sending sensitive information via Wi-Fi*	HAISQ, RSCB	Masquerade by outsiders
3.8	Sharing sensitive information/posting about work on social media*	HAISQ, RSCB	Masquerade by outsiders
3.9	Reporting all incidents	HAISQ	User error, technical failure
3.10	Ignoring poor security behavior by colleagues*	HAISQ	User error, misuse of system resources
4.1	Disposing of sensitive printouts properly.	HAISQ	Theft by outsiders
4.2	Never leaving sensitive material.	HAISQ	Theft by outsiders

CODE	ISB INDICATORS	SECURITY BEHAVIOR FRAMEWORK	INFORMATION SECURITY THREATS IN HOSPITAL
4.3	Backing up data files as frequently as possible	CCSB	Maintenance error, application software failure
4.4	Not always treating sensitive data carefully*	RSCB, CCSB	User error
4.5	Sending personal information to strangers (through instant messaging)*	RSCB	User error
4.6	Sending personal information to strangers (through a website)*	RSCB	User error

*Reversed items

Phase 2. Quantitative study: Measuring security behavior based on security threats

We collected data using questionnaires online and offline from hospital employees and got 144 responses. After validating the data, only 125 responses completed the questionnaire, which could be analyzed further. Table 7 shows the respondents' demographics. Most of the respondents are female (71%), nurse/pharmacist (34%), 30–39 years (33%), and undergraduate level (60%).

Table 7. Demographics of survey respondents

CHARACTERISTICS		FREQUENCY
Profession	Nurse/pharmacist	43
	Other health professionals (nutritionists, physiotherapists, health information.)	41
	Doctor/dentist/resident	24
	Administration staff	17
Gender	Female	89
	Male	36
Age	18 - 29 years	33
	30 - 39 years	41
	40 - 49 years	20
	>50 years	31
Education	High-school	5
	Diploma	28
	Undergraduate	75
	Post-graduate	17

Validity and reliability test

The result of the Cronbach Alpha value for 28 items is 0.738 (see Table 8). It means that the survey instrument is reliable. Meanwhile, four items (1.6, 2.6, 3.5, 3.10) needed to meet the validity test criteria. Therefore, we conducted the second test after excluding those items. The second step validity test result (Table 9) shows that all items were valid and could be processed to the next step.

Table 8. Reliability test results

TEST NUMBER	CRONBACH'S ALPHA	N OF ITEMS
First test	0.738	28
Second test	0.791	24

Table 9. Validity test results

INDICATOR	FIRST-ROUND TEST (N=28)		SECOND ROUND TEST (N=24)	
	SIG. (2-TAILED)	PEARSON CORRELATION	SIG. (2-TAILED)	PEARSON CORRELATION
1.1	0.000	0.481**	0.000	0.518**
1.2	0.000	0.421**	0.000	0.463**
1.3	0.000	0.433**	0.000	0.482**
1.4	0.000	0.433**	0.000	0.409**
1.5	0.014	0.220*	0.023	0.204*
1.6	0.783	-0.025	-	-
2.1	0.000	0.537**	0.000	0.560**
2.2	0.000	0.433**	0.000	0.465**
2.3	0.000	0.427**	0.000	0.418**
2.4	0.000	0.428**	0.000	0.414**
2.5	0.000	0.372**	0.000	0.342**
2.6	0.534	0.056	-	-
3.1	0.000	0.503**	0.000	0.516**
3.2	0.000	0.518**	0.000	0.551**
3.3	0.002	0.271**	0.000	0.320**
3.4	0.000	0.410**	0.000	0.464**
3.5	0.162	0.126	-	-
3.6	0.000	0.413**	0.000	0.384**
3.7	0.000	0.331**	0.000	0.320**
3.8	0.001	0.304**	0.001	0.285**
3.9	0.000	0.628**	0.000	0.660**
3.10	0.202	0.115	-	-
4.1	0.000	0.601**	0.000	0.629**
4.2	0.000	0.341**	0.000	0.355**
4.3	0.000	0.413**	0.000	0.447**
4.4	0.003	0.265**	0.044	0.180*
4.5	0.016	0.215*	0.022	0.205*
4.6	0.000	0.318**	0.000	0.316**

** Correlation is significant at the 0.01 level (2-tailed).

* Correlation is significant at the 0.05 level (2-tailed).

Figure 2 shows that the HIS users in the hospital already have good, desirable security behavior, especially in verifying link sources, disposing of printouts properly, and never leaving sensitive documents in unsupervised areas. Meanwhile, the staff rarely change passwords, lock workstations, and verify websites before sending sensitive information. Figure 2 also describes the staff's security behavior in updating software, logging out after using the system, and sending sensitive information through public Wi-Fi is still frequently done and needs improvement.

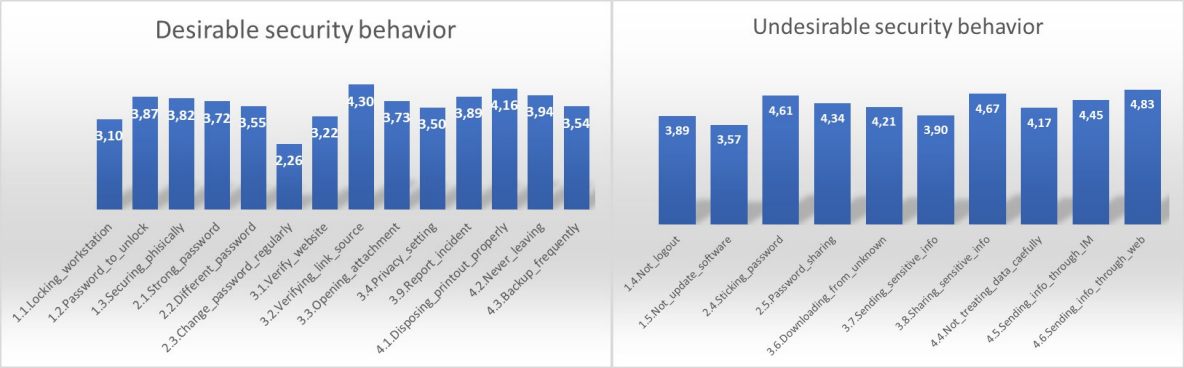

Figure 2. Healthcare professionals' information security behavior assessment

Table 10 shows the description of each security behavior in more detail. Most HIS users always practice the ideal security behavior, which includes validating the source before clicking on a link (54.4%) and ensuring sensitive document printouts are destroyed adequately before disposal (55.2%). Changing passwords regularly is a security practice that is currently uncommon (34.4% of users have yet to practice it). Meanwhile, many hospital staff never lock their electronic devices (26.4%) when they are not using HIS, but this percentage is balanced by users who consistently lock their devices (25.6%). Sending personal information to strangers through websites (86.4%), writing passwords in open areas (79.2%), and posting sensitive information on social media (76.8%) are all examples of undesirable security behavior that the majority of HIS users practically never engage in. However, HIS users frequently engage in risky behavior, such as not logging out after using the system (7.2%) and mishandling sensitive data with care (7.2%).

Table 10. Descriptive security behavior indicators

CODE	INDICATOR	FREQUENCY (%)				
Desirable security behavior		**Never**	**Seldom**	**Sometime**	**Often**	**Always**
1.1	Locking_workstation	26.4	12.0	12.0	24.0	25.6
1.2	Password_to_unlock	14.4	7.2	6.4	20.8	51.2
1.3	Securing_phisically	8.8	9.6	13.6	26.4	41.6
2.1	Strong_password	16.0	11.2	7.2	16.0	49.6
2.2	Different_password	12.0	18.4	9.6	22.4	37.6
2.3	Change_password_regularly	34.4	28.0	19.2	13.6	4.8
3.1	Verify_website	13.6	19.2	20.0	26.4	20.8
3.2	Verifying_link_source	2.4	4.8	8.0	30.4	54.4
3.3	Opening_attachment	5.6	14.4	14.4	32.8	32.8
3.4	Privacy_setting	6.4	13.6	26.4	30.4	23.2
3.9	Report_incident	5.6	11.2	16.8	21.6	44.8
4.1	Disposing_printout_properly	3.2	10.4	8.8	22.4	55.2
4.2	Never_leaving	12.0	8.0	4.8	24.8	50.4
4.3	Backup_frequently	12.0	8.8	22.4	26.4	30.4
Undesirable security behavior		**Always**	**Often**	**Sometime**	**Seldom**	**Never**
1.4	Not_logout	7.2	11.2	16.0	16.8	48.8
1.5	Not_update_software	4.8	12.8	25.6	34.4	22.4
2.4	Sticking_password	1.6	4.8	4.0	10.4	79.2

CODE	INDICATOR	FREQUENCY (%)				
2.5	Password_sharing	1.6	3.2	13.6	23.2	58.4
3.6	Downloading_from_unknown	0.0	6.4	15.2	29.6	48.8
3.7	Sending_sensitive_info	1.6	9.6	23.2	28.0	37.6
3.8	Sharing_sensitive_info	0.0	2.4	4.8	16.0	76.8
4.4	Not_treating_data_carefully	7.2	3.2	10.4	24.0	55.2
4.5	Sending_info_through_IM	0.8	7.2	5.6	19.2	67.2
4.6	Sending_info_through_web	0.0	0.8	1.6	11.2	86.4

Phase 3. Qualitative study: Investigating the factors that influence security behaviors

After getting the description of hospital staff's security behavior, the next step of this study was finding the explanation of why they do or do not practice HIS security protection. We randomly selected 13 respondents (10% of the sample in the quantitative study) from the survey and asked for their permission to be interviewed. Firstly, we selected two persons from each profession. Since most respondents were female, we randomly chose seven females and six males in the second selection. Then, among those candidates of respondents, we chose age and education level accordingly. Two respondents rejected to be interviewed. The information on interviewees' characteristics can be seen in Table 11.

Table 11. Interviewees' characteristics

CODE	PROFESSION	GENDER	AGE (YEARS)	EDUCATION LEVEL
IN1	Administration staff	Male	30 - 39	Post-graduate
IN2	Other health professionals	Male	40 - 49	Undergraduate
IN3	Doctor/dentist/resident	Male	50 - 59	Post-graduate
IN4	Doctor/dentist/resident	Female	30 - 39	Undergraduate
IN5	Nurse/pharmacist	Female	40 - 49	Diploma
IN6	Doctor/dentist/resident	Male	18 - 29	Undergraduate
IN7	Administration staff	Female	40 - 49	Undergraduate
IN8	Nurse/pharmacist	Female	50 - 59	Post-graduate
IN9	Other health professionals	Male	50 - 59	Diploma
IN10	Nurse/pharmacist	Female	40 - 49	Post-graduate
IN11	Doctor/dentist/resident	Male	18 - 29	Undergraduate

We processed the interview transcripts using thematic coding analysis to map with variables in PMT and GDT as influencing factors of information security behavior. GDT's variables were management support, security monitoring, and information security regulation awareness. Variables from PMT were perceived benefit, perceived barrier, perceived severity, and perceived susceptibility. In addition, from these attributes, this study investigated other factors that might impact staff information security behavior in hospitals. We discovered that workload situations, such as emergency conditions or high patient visits, impact users who engage in risky behaviors. Healthcare workers emphasize patient services; thus, security measures seen as slowing down treatment were frequently abandoned in this circumstance. Table 12 describes each of these characteristics at the hospital based on the interview results.

Table 12. Influential factors to health workers' information security behavior

INFLUENTIAL FACTORS	DESCRIPTION	INTERVIEWEE'S NOTE
Management Support	Management provides guidelines for implementing HIS in hospitals, especially for user access control to support information security.	"*There is a Director's Decree regarding user access rights.*" [N1]
	Management delivers HIS training, emphasizing system filling and access control management. There is no special training available to raise staff awareness regarding information security.	*"There is no official training. (about information security). There is simply a manual for using EMR"*[N5]
	Management support in the form of policies and SOP to regulate the usage of HIS is considered insufficient. Management must monitor and evaluate policies to ensure they operate as planned.	"*Policies and SOPs already exist, but there is no monitoring and evaluation to ensure everything is running.*" [N10]
	Management has to develop more specific procedures for information security protection. This policy can then be simplified to technical protection determined by the system's requirements.	*"Each application requires different security protection, so management needs clear directions in the form of policies.*" [N8]
Security monitoring	All hospital-owned equipment and the user's devices to access the system and network must be registered with the IT Department for security monitoring.	*"The IT unit monitors the registration of devices that will connect to Wi-Fi."* [N7]
	The IT Department monitors the security of all devices registered to the hospital network.	*"There is Internet use monitoring; if a user has downloaded a lot, access will be slowed down.*" [N4]
Regulatory awareness	The employee stated several laws about information security in general and in the health industry, notably the Electronic Information and Transaction Law and the Ministry of Health regulations regarding Medical Records.	*"UU ITE, especially related to behavior in using social media.*" [N1] *"Regulation of the Minister of Health No 24 of 2022 concerning Medical Records.*" [N2]
	The government has adopted new laws on medical records, including establishing an information security system that healthcare providers must employ. However, the source stated that the regulation was insufficient; thus, additional measures were required.	*"For example, every health facility must have an information security system, but it is unclear which type is required.*" [N4]
Perceived benefit	Limiting access to HIS promotes a sense of security and trust in patient data stored within the system.	*"Trust in patient information stored because only authorized users can access.*" [N3]
	Clear regulations can help healthcare facility managers adopt HIS information security.	*"Provide guidance on implementing information security in health facilities"* [N10]
	Information security ensures that patient data will be more secure.	*"Outsiders are more difficult to see patient data.*" [N6]
Perceived severity	As there is no penalty mechanism for users who create security problems, many users continue to engage in actions that risk creating incidents, such as not logging out of the system after using it.	*"By regulation, there is punishment in the form of a warning letter. However, it has not been fully implemented.*" [N3]
	Users are still tolerant of the present security issue. For example, when a system outage happens, the user will use manual methods.	*"If the system cannot be accessible, the pharmacy unit supplies handwritten paperwork for medication prescriptions."* [N10]

INFLUENTIAL FACTORS	DESCRIPTION	INTERVIEWEE'S NOTE
	The impact of the problem resulted in a delayed service process since users could not access the system.	*"Performance is hampered, for example, by the inability to retrieve data stored on an infected device."* [N7]
Perceived barrier	Layered login methods (password and captcha) are thought to slow down users' ability to access data on the system, particularly during emergencies.	*"… the use of captcha for login hinders access to the system, especially during emergency conditions that require fast time."* [N4]
	Automatic logout will likely delay the process since the user must re-login while the system is utilized to provide patient services.	*"The automatic logout system requires the user to log in repeatedly so that it takes longer."* [N6]
	Separating roles to review data before it gets delivered to patients is considered a barrier to the service process.	*"Due to the large quantity of data that must be cross-checked, nurses frequently exchange passwords to speed up the procedure."* [N4]
Perceived susceptibility	Changes in system status without notification put users at risk of making mistakes while reading or inputting patient data, which can lead to misdiagnosis and poor patient care.	*"A warning system is required if the status has changed due to a stressful work environment, as users are sometimes not cautious."* [N6]
	Because antivirus is not offered for devices that do not belong to the hospital, the user's device used to access HIS is in danger of getting infected by malware.	*"For personal laptops, you must provide your antivirus."* [N4]
Workload situation	Users emphasize health services to patients during busy periods; thus, they leave the workstation without first locking it.	*"The employee leaves the workstation without logging out of the system first."* [N3]
	In an emergency, users tend to put off entering HIS data to provide immediate patient care.	*"When a patient's condition changes quickly, data input must be done outside of real time."* [N5]
	Doctors cannot access devices to open patient data in HIS while treating patients; hence they delegate access to assistants/nurses.	*"Sharing passwords to speed up service."* [N4]

DISCUSSION

We found that the hospital has established nine of 14 security control clauses in ISO 27799:2016 (as seen in Table 3). The information security policy is part of the hospital's overall policy for deploying health information systems. The Indonesian government encourages hospitals to implement ISMS through regulations concerning electronic medical records and hospital information systems. Addressing national (Hospital Accreditation Committee/KARS) and international (Joint Commission International/JCI) hospital standards also triggers hospitals to execute this strategy. JCI and KARS accreditation requirements encourage hospitals to adopt health information system policies. The accreditation standard requires the accuracy of user access rights, the availability of data at all times, the fulfillment of data requirements for each stakeholder, the organization structures of IT management, data integration, data completeness, and the role of each actor such as user, management, and IT department. Despite knowing that security requirements already exist in Hospital Accreditation standards, surveyors are often health personnel who must assess information security more thoroughly.

This result revealed that insider masquerade had become the majority of information security threats in the hospital, followed by user mistakes, unauthorized use of HISs, abuse of system resources, application failure, and maintenance error as internal sources. Medical workers exchange their

usernames and passwords with other users to assist them in accessing patient data at HIS since job conditions do not allow them to access devices when treating patients. Masquerade by insiders also occurs to speed up work operations when patient visits are high, but HIS security requirements necessitate data submission by distinct users. In addition, HIS management also needs to anticipate external threats such as masquerade by outsiders, malware, theft by outsiders, and technical problems caused by power failure. It is supported by the prior study in Malaysia (Samy et al., 2010) that found major critical threats for HIS are power failure, human error, and technological problems. Another study in Dubai (Bakkar & Alazab, 2019) confirms that common security threats in hospitals are people threats and power failure. It indicates that lower-middle-income countries (such as Indonesia), upper-middle-income countries (such as Malaysia), and high-middle-income countries (such as the United Arab Emirates) deal with nearly identical information security vulnerabilities connected to HIS, specifically the people threat. It is supported by a previous study's experiment (Preistman et al., 2019) that hospital employee credential information has become a primary target of cyberattacks. As a result, this study undertakes the additional examination of HIS users' ISB, which is the primary vector of the threat.

The overall results show that health professionals in the hospital have implemented good ISB on protecting HIS access devices, password management, handling sensitive information, and protecting information assets in general communication channels (Internet, e-mail, social media, and instant messaging). Most HIS users in hospitals are medical workers who are obligated by a code of ethics to protect the privacy and confidentiality of patient data. They will be cautious when it comes to the handling of sensitive patient data. However, their hectic schedule of providing services to patients leads them to leave the workstation or the system open occasionally, and some sensitive data needs to be protected correctly. A previous study in different hospitals in Indonesia (Fauzi et al., 2021) revealed that the riskiest behavior is viewing external websites using the hospital's computer, while the least risky is uploading patient information on social media. It is not supported by this study, where sharing sensitive information on social media is one of the top three undesirable security behaviors that rarely occur on average. In other words, health professionals participate in the least harmful behavior. Meanwhile, because it failed the validity test, visiting suspicious websites is not analyzed further in this study. Another study (Aljedaani et al., 2020) implies that most mHealth end-users prefer to keep the app's password the same. According to this study, updating passwords regularly is the least prevalent security behavior among health workers. It implies that ordinary users and health workers have the same weaknesses in password management security, suggesting that HIS administrators must incorporate additional security measures to anticipate threats from this side. Hospital management and HIS administrators must also be aware of the factors that might impact the ISB of health workers in order to give adequate control and education.

The outcomes of this study demonstrate that health professionals' ISB is impacted by their beliefs of the benefit of security protection, the severity of the impact of an incident, the barrier to implementing security measures, and vulnerability to malware and system malfunction. However, the benefit of security controls is still dominated by confidentiality aspects related to HIS access limitation only for authorized users. The staff are still tolerant of the security risk because they will resort to manual procedures if a system fails. Similar to the previous study's findings (Bakkar & Alazab, 2019), HIS availability will not become a priority since nurses still perform operations manually. Moreover, through establishing security policies, procedures, and education to define information security in the hospital, management support also impacts the ISB. Other factors mentioned by respondents include security monitoring performed by the IT Department on all registered devices and the hospital network and staff awareness of government regulations regarding HIS information security. The previous study in the financial sector (Carmi & Bouhnik, 2020) also demonstrated a tight relationship between information security policy conduct and personal consequences due to actions deriving directly from the employees' behavior.

This study also revealed that in some circumstances related to their workloads, such as patient emergencies or many visits, sharing passwords is considered a desirable security behavior since it can speed up work. Nurses, for example, can use the doctor's account to substitute doctors who assess patients to open data in HIS since access to patient medical record data is only granted to doctors who offer services. It is supported by staff who only update passwords occasionally. Nurses can use the same password for an extended time without confirming it with the doctor. Previous research (Bulgurcu et al., 2010) claimed that when workers believe that following information security procedure will impede their capacity to work, they may participate in non-compliance actions. Some security requirements need to be more adequately implemented using current security mechanisms. When the system is inactive, the two-authentication factor at the login procedure and the automated logout feature are thought to slow down access to HIS, particularly in emergencies. Segregation of duties to examine data accuracy, such as cross-checking for medicine doses, is sometimes deemed to impede service because it is performed by other personnel who are simultaneously on duty delivering services in other units. It encourages employees to exchange passwords with colleagues for self-validation. Previous research (Burns, 2021) has found that employees' desire to protect information assets is heavily impacted by their view of the benefits of not protecting or following security procedures. Furthermore, this conduct is regarded as legitimate because most employees practice it. According to Hwang et al. (2017), employees develop routines based on the habits of their peers in order to reduce the unpredictability of their operations.

The study's findings have implications for theory in information security, particularly in healthcare organizations. This research examines the theoretical frameworks of PMT and GDT, which are only partially relevant to health organizations in developing countries that lack effective information security rules and regulations. Furthermore, this study discovered signs of alternative theoretical grounds that may be used to explore information security behavior that is impacted by different work settings and the influence of peers at work.

Conclusion, Contribution, and Future Works

This study examines the IT implementation policy of the National Cardiovascular Center Harapan Kita in Indonesia, a specialized public hospital with a positive evaluation for information security, to analyze healthcare trends and performance. This study was conducted in three phases. The first phase used qualitative research to investigate hospital information security threats and controls, utilizing interviews with IT and Medical Record departments. Data was analyzed using first-cycle and second-cycle coding techniques, identifying implemented security protection and risks. This second phase used the modified SeBIS framework to measure hospital security behavior. Data was collected through surveys with medical and non-medical staff. Descriptive statistics and reliability tests were conducted, with a higher mean value indicating better ISB. The third phase used a qualitative study to explore the influence of information security behavior on established security controls, utilizing semi-structured interviews and thematic coding analysis to identify patterns and themes. This phase aimed to provide a deeper understanding of how security behavior impacts the effectiveness of security controls in hospitals. The findings from this qualitative study can then be used to enhance and improve the overall security protection measures in healthcare organizations.

This study provides academics and policymakers in comparable healthcare organizations with knowledge about the ISB of health workers and the underlying elements that influence their ISB. This research can potentially improve information security in the healthcare industry, which poses significant dangers to human life but lags behind other critical industries in implementation. Hospital management can improve HIS information security design by automatically locking hospital devices, performing regular software updates, automatic password renewal for a set period, making the initial password for new users a one-time password, filtering sites that may contain malware, ensuring the data backup process is carried out regularly, a feature to reset password to encourage users to change

passwords regularly, and more efficient data validation process to minimize sharing password intention among staffs. HIS managers could incentivize employees to increase their opinions of the benefits of information security procedures. Practical training, such as direct education by providing examples of information security practices to users or indirect teaching via infographics, is required to increase employee comprehension and awareness of security rules and controls. Although this study was conducted in Indonesia, many other middle-income nations have comparable ISMS limitations, and the conclusions from this study may be beneficial.

This study has some limitations. First, this study solely employs case studies from one public hospital, which may have superior resource circumstances than general healthcare institutions in Indonesia. Second, based on PMT and GDT theory, this study solely looks at the elements that impact information security behavior from the perspective of HIS users. More antecedents must be investigated from the standpoint of various stakeholders and theories in order to generate more complete conclusions. Another theoretical underpinning, such as Regulatory Focus Theory (RFT), can be used to compare preventive and promotion motivation to influence desirable security behavior. RFT has never been employed in studies of information security behavior in healthcare organizations (Sari et al., 2022). Previous studies utilizing this theory in contexts other than healthcare have found that promotion-focused and prevention-focused approaches can directly influence information security behavior preferences (Shih et al., 2021) or indirectly (Burns, 2021; Hwang & Cha, 2018). Future studies might also look at the most suitable material and structure for an information security education and training program to encourage healthcare professional behaviors that need to be changed based on this ISB assessment and influential factors.

ACKNOWLEDGMENT

We would like to thank Universitas Indonesia for their support through PUTI Pascasarjana Grants (No. NKB-023/UN2.RST/HKP.05.00/2023).

REFERENCES

Ahouanmenou, S., Van Looy, A., & Poels, G. (2022). Information security and privacy in hospitals: A literature mapping and review of research gaps. *Informatics for Health and Social Care*, *48*(1), 30-46. https://doi.org/10.1080/17538157.2022.2049274

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

Aljedaani, B., Ahmad, A., Zahedi, M., & Babar, M. A. (2020). Security awareness of end-users of mobile health applications: An empirical study. *Proceedings of the 17th EAI International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services* (pp. 125–136). Association for Computing Machinery. https://doi.org/10.1145/3448891.3448952

Badan Siber dan Sandi Negara. (2022). *Lanskap Keamanan Siber Indonesia 2022*.[Indonesia's cybersecurity landscape 2022]. https://www.bssn.go.id/lanskap2022/

Bakkar, M., & Alazab, A. (2019, May). Information security: Definitions, threats and management in Dubai hospitals context. *Proceedings of the Cybersecurity and Cyberforensics Conference, Melbourne, Australia,* 152–159. https://doi.org/10.1109/CCC.2019.00010

Brady, J. W. (2011, January). Securing health care: Assessing factors that affect HIPAA security compliance in academic medical centers. *Proceedings of the Hawaii International Conference on System Sciences*, *Kauai, HI*, *USA*, 1–10. https://doi.org/10.1109/HICSS.2011.368

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly*, *34*(3), 523–548. https://doi.org/10.2307/25750690

Burhan, F. A. (2020). *Data Pasien Covid-19 Bocor Dianggap Tanggung Jawab Kemenkes*. [Leaking Covid-19 patient data is considered the responsibility of the Ministry of Health]. https://katadata.co.id/yuliawati/digital/5f02f85af052d/data-pasien-covid-19-bocor-dianggap-tanggung-jawab-kemenkes

Burns, A. J. (2021, January). Protecting organizational information assets: Exploring the influence of regulatory focus on rational choices. *Proceedings of the 54th Hawaii International Conference on System Sciences*, *Maui, Hawaii, USA,* 5228–5237. https://doi.org/10.24251/hicss.2021.637

Calyptix. (2018). *Top 5 cyber security frameworks in healthcare*. https://www.calyptix.com/hipaa/top-5-cyber-security-frameworks-in-healthcare/

Carmi, G., & Bouhnik, D. (2020). The effect of rational based beliefs and awareness on employee compliance with information security procedures: A case study of a financial corporation in Israel. *Interdisciplinary Journal of Information, Knowledge, and Management*, *15*, 109–125. https://doi.org/10.28945/4596

CNN-Indonesia. (2020). *230 Ribu Data Pasien Covid-19 di Indonesia Bocor dan Dijual*. https://www.cnnindonesia.com/teknologi/20200620083944-192-515418/230-ribu-data-pasien-covid-19-di-indonesia-bocor-dan-dijual

Coventry, L., & Branley, D. (2018). Cybersecurity in healthcare: A narrative review of trends, threats and ways forward. *Maturitas*, *113*, 48–52. https://doi.org/10.1016/j.maturitas.2018.04.008

D'Arcy, J., Hovav, A., & Galletta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. *Information System Research*, *20*(1), 79–98. https://doi.org/10.1287/isre.1070.0160

Dreyfuss, M., & Giat, Y. (2016, June). Identifying security risk modules in a university's information system. *Proceedings of the Informing Science & IT Education Conference*, *Vilnius, Lithuania,* 41–51. https://doi.org/10.28945/3436

Egelman, S., & Peer, E. (2015). Predicting privacy and security attitudes. *SIGCAS Computers and Society*, *45*(1), 22–28. https://doi.org/10.1145/2738210.2738215

Fatima, A., & Colomo-Palacios, R. (2018). Security aspects in healthcare information systems: A systematic mapping. *Procedia Computer Science*, *138*, 12–19. https://doi.org/10.1016/j.procs.2018.10.003

Fauzi, M. A., Yeng, P., Yang, B., & Rachmayani, D. (2021). Examining the link between stress level and cybersecurity practices of hospital staff in Indonesia. *Proceedings of the 16th International Conference on Availability, Reliability and Security*. Association for Computing Machinery. https://doi.org/10.1145/3465481.3470094

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*(6), 454–467. https://doi.org/10.1016/j.ijmedinf.2015.01.010

Foth, M. (2016). Factors influencing the intention to comply with data protection regulations in hospitals: Based on gender differences in behaviour and deterrence. *European Journal of Information Systems*, *25*(2), 91–109. https://doi.org/10.1057/ejis.2015.9

Foth, M., Schusterschitz, C., & Flatscher-Thöni, M. (2012). Technology acceptance as an influencing factor of hospital employees' compliance with data-protection standards in Germany. *Journal of Public Health*, *20*(3), 253–268. https://doi.org/10.1007/s10389-011-0456-9

Hadlington, L. (2017). Human factors in cybersecurity; examining the link between internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. *Heliyon*, *3*(7), E00346. https://doi.org/10.1016/j.heliyon.2017.e00346

Hwang, I., & Cha, O. (2018). Examining technostress creators and role stress as potential threats to employees' information security compliance. *Computers in Human Behavior*, *81*, 282–293. https://doi.org/10.1016/j.chb.2017.12.022

Hwang, I., Kim, D., Kim, T., & Kim, S. (2017). Why not comply with information security? An empirical approach for the causes of non-compliance. *Online Information Review*, *41*(1), 2–18. https://doi.org/10.1108/OIR-11-2015-0358

Ifinedo, P., & Akinnuwesi, B. A. (2014, October). Employees' non-malicious, counterproductive computer security behaviors (CCSB) in Nigeria and Canada: An empirical and comparative analysis. *Proceedings of the IEEE 6th International Conference on Adaptive Science & Technology*, *Ota, Nigeria,* 1–7. https://doi.org/10.1109/ICASTECH.2014.7068109

International Organization for Standardization (ISO). (2016). *ISO 27799: Health informatics – Information security management in health using ISO/IEC 27002*. https://www.iso.org/standard/62777.html

Interpol. (2020, April 4). *Cybercriminals targetting critical healthcare institutions with ransomware*. https://www.interpol.int/en/News-and-Events/News/2020/Cybercriminals-targeting-critical-healthcare-institutions-with-ransomware

Jercich, K. (2021). *VMware Carbon Black's healthcare users faced 239M attempted cyberattacks in 2020*. https://www.healthcareitnews.com/news/vmware-carbon-blacks-healthcare-users-faced-239m-attempted-cyberattacks-2020

Johnston, A. C., & Warkentin, M. (2008). Information privacy compliance in the healthcare industry. *Information Management & Computer Security*, *16*(1), 5–19. https://doi.org/10.1108/09685220810862715

Kertopati, L. (2017). *Dua Rumah Sakit di Jakarta Kena Serangan Ransomware WannaCry*. [Two hospitals in Jakarta hit by WannaCry Ransomware]. https://www.cnnindonesia.com/teknologi/20170513191519-192-214642/dua-rumah-sakit-di-jakarta-kena-serangan-ransomware-wannacry

Kumparan. (2020). *Data Pasien Corona Indonesia yang Dibobol Hacker: Nama, Alamat, hingga Hasil Tes*. [Data on Indonesian corona patients hacked by hackers: Names, addresses, and test results]. https://kumparan.com/kumparantech/data-pasien-corona-indonesia-yang-dibobol-hacker-nama-alamat-hingga-hasil-tes-1teOFqCfniX/full

Layman, E. J. (2008). Ethical issues and the electronic health record. *Health Care Manager*, *27*(2), 165–176. https://doi.org/10.1097/01.HCM.0000285044.19666.a8

Liginlal, D., Sim, I., Khansa, L., & Fearn, P. (2012). HIPAA Privacy Rule compliance: An interpretive study using Norman's action theory. *Computers & Security*, *31*(2), 206–220. https://doi.org/10.1016/j.cose.2011.12.002

Ndibwile, J. D., & Luhanga, E. T. (2018). Smart4Gap: Factors that influence smartphone security decisions in developing and developed countries. *Proceedings of the 10th International Conference on Information Management and Engineering* (pp. 5–15). Association for Computing Machinery. https://doi.org/10.1145/3285957.3285980

Norman, P., Boer, H., & Seydel, E. R. (2005). Protection motivation theory. In M. Conner & P. Norman (Eds.), *Predicting health behaviour* (2nd ed., pp. 81–126). Open University Press.

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

Oltsik, J. (2020). The impact of the COVID-19 pandemic on cybersecurity. *ESG Research Report,* https://www.issa.org/wp-content/uploads/2020/07/ESG-ISSA-Research-Report_COVID-19-Jul-2020.pdf

Ozair, F. F., Jamshed, N., Sharma, A., & Aggarwal, P. (2015). Ethical issues in electronic health records: A general overview. *Perspectives in Clinical Research*, *6*(2), 73–76.

Park, E. H., Kim, J., & Park, Y. S. (2017). The role of information security learning and individual factors in disclosing patients' health information. *Computers & Security*, *65*, 64–76. https://doi.org/10.1016/j.cose.2016.10.011

Park, E. H., Kim, J., Wiles, L. L., & Park, Y. S. (2018). Factors affecting intention to disclose patients' health information. *Computers & Security*, *87*, 101340. https://doi.org/10.1016/j.cose.2018.05.003

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

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

Pathania, A., & Rasool, G. (2019). Investigating power styles and behavioural compliance for effective hospital administration: An application of AHP. *International Journal of Health Care Quality Assurance*, *32*(6), 958–977. https://doi.org/10.1108/IJHCQA-02-2018-0059

PERSI. (2022). *PERSI dan BSSN Kupas Isu-Isu Terkini Keamanan Siber di RS, Menanti Regulasi dan Pemahaman Manajemen*. [PERSI and BSSN discuss latest cybersecurity issues in hospitals, waiting for regulations and management understanding]. Persi.or.Id. https://persi.or.id/persi-dan-bssn-kupas-isu-isu-terkini-keamanan-siber-di-rs-menanti-regulasi-dan-pemahaman-manajemen/

Pollini, A., Callari, T. C., Tedeschi, A., Ruscio, D., Save, L., Chiarugi, F., & Guerri, D. (2022). Leveraging human factors in cybersecurity: an integrated methodological approach. *Cognition, Technology and Work*, *24*, 371–390. https://doi.org/10.1007/s10111-021-00683-y

Preistman, W., Anstis, T., Sebire, I. G., Sridharan, S., & Sebire, N. J. (2019). Phishing in healthcare organisations: Threats, mitigation and approaches. *BMJ Health & Care Informatics*, *26*, e100031. https://doi.org/10.1136/bmjhci-2019-100031

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

Saldaña, J. (2013). *The coding manual for qualitative researchers* (2nd ed.). Sage.

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

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

Sawaya, Y., Sharif, M., Christin, N., & Kubota, A. (2017). Self-confidence trumps knowledge: A cross-cultural study of security behavior. *Proceedings of the CHI Conference on Human Factors in Computing Systems* (pp. 2202–2214). Association for Computing Machinery. https://doi.org/10.1145/3025453.3025926

Schmidt, T., Nøhr, C., & Koppel, R. (2021). A simple assessment of information security awareness in hospital staff across five Danish regions. *Studies in Health Technology and Informatics*, *281*, 635–639. https://doi.org/10.3233/SHTI210248

Sher, M.-L., Talley, P. C., Cheng, T.-J., & Kuo, K.-M. (2017). How can hospitals better protect the privacy of electronic medical records? Perspectives from staff members of health information management departments. *Health Information Management Journal*, *46*(2), 87–95. https://doi.org/10.1177/1833358316671264

Shih, H. P., Lai, K. H., Guo, X., & Cheng, T. C. E. (2021). Believe it or not: Employees intend to comply with information security policy because of the desire for trade-offs. *Journal of Global Information Management*, *29*(6). https://doi.org/10.4018/JGIM.294329

Straub, D. W., & Welke, R. J. (1998). Coping with systems risk: Security planning models for management decision making. *MIS Quarterly*, *22*(4), 441–469. https://doi.org/10.2307/249551

Tidy, J. (2020). *Police launch homicide inquiry after German hospital hack*. https://www.bbc.com/news/technology-54204356

Tonkin, C. (2021). *Australian hospitals hit by cyber attack*. https://ia.acs.org.au/article/2021/australian-hospitals-hit-by-cyber-attack.html

Zikmund, W., Babin, B., Carr, J., & Griffin, M. (2010). *Business research methods* (8th ed.). Cengage Learning.

AUTHORS

Puspita Kencana Sari is an assistant professor at the Faculty of Economics and Business, Telkom University. She received her doctorate degree in Computer Science from the Faculty of Computer Science, University of Indonesia. Her research interest is related to information security management, IS user behavior, e-commerce and e-health.

Putu Wuri Handayani is a professor at the Faculty of Computer Science, University of Indonesia. She received her doctorate degree in Computer Science from the Faculty of Computer Science, University of Indonesia. Her research interests are related to e-commerce and e-health system design and behavioral analysis (both quantitative and qualitative). She is also a member of the IT steering committee at Hermina Hospitals Group, Indonesia.

Achmad Nizar Hidayanto is a professor in Information Systems at the Faculty of Computer Science, Universitas Indonesia. He is also a Vice Dean for Resources, Venture, and General Administration. He received his bachelor's degree, master's degree and Ph.D. degree in computer science from the Universitas Indonesia in 1999, 2002, and 2008 respectively. His research interests are related to e-health, information systems/information technology management, e-commerce, e-government, information systems security, and information systems/information technology adoption.

Pribadi Wiranda Busro is a cardiothoracic surgeon at the National Cardiovascular Center Harapan Kita (RSPJNHK). He is also an assistant professor in the Faculty of Medicine, University of Indonesia. He received his doctorate degree in the Faculty of Medicine, University of Indonesia. He is also Head of Medical Service Quality Improvement and Control in RSJPNHK. His research interest is pediatric cardiac surgery.