**Early Version – Uncorrected**




# Assessing Information Security Awareness among Electronic Medical Records Personnel in Indonesia: A Preliminary Validation of the HAIS-Q

Titin Wahyuni, Ervita Nindy Oktoriani, Diah Wijayanti Sutha, Yuni Sari Amalia

DOI: http://dx.doi.org/10.31584/jhsmr.20261508

Received: 26 December 2025

Revised: 3 April 2026

Accepted: 23 May 2026

Published online: 12 November 2026

Please cite this article as: Wahyuni T, Oktoriani EN, Sutha DW, Amalia YS. Assessing information security awareness among electronic medical records personnel in Indonesia: a preliminary validation of the HAIS-Q. J Health Sci Med Res 2026 doi: http://dx.doi.org/10.31584/jhsmr.20261508

Early Version — Uncorrected: This accepted manuscript has not been typeset or proofread. Content and formatting may change prior to final publication and should not be regarded as the final Version of Record.

© 2026 JHSMR. Hosted by Prince of Songkla University.

This is an open access article under the CC BY-NC-ND license (https://creativecommons.org/licenses/by-nc-nd/4.0/).

**Original Article**

# Assessing Information Security Awareness among Electronic Medical Records Personnel in Indonesia: A Preliminary Validation of the HAIS-Q

Titin Wahyuni, M.Kes[1], Ervita Nindy Oktoriani, M.AB[2], Diah Wijayanti Sutha[1], Yuni Sari Amalia, Ph.D.[3]

[1]STIKES Yayasan RS Dr. Soetomo - Medical Records and Health Information Jl. Kalidami 14-16, Surabaya 60285 Indonesia.
[2]STIA Malang Ringgold standard institution - Medical Records and Health Information Bulan Baiduri 1, Tlogomas, Lowokwaru, Malang, Indonesia, Malang, East Java 65144 Indonesia.
[3]Airlangga University Ringgold standard institution - Faculty of Humanities Dharmawangsa Dalam, Surabaya, East Java 60115, Indonesia.

**Corresponding Author**
**Contact:** Titin Wahyuni, M.Kes,
STIKES Yayasan RS Dr. Soetomo – Medical Records and Health Information Jl. Kalidami 14-16, Surabaya 60285 Indonesia.
**E-mail:** titin@stikes-yrsds.ac.id

Early Version - Uncorrected

**ABSTRACT**

**Objective**: This study aimed to evaluate preliminary evidence of the validity and internal consistency of the Indonesian version of the Human Aspects of Information Security Questionnaire (HAIS-Q) and to assess information security awareness among medical records personnel using electronic medical records (EMR) systems.

**Material and Methods:** A cross-sectional pilot study was conducted involving 52 medical records personnel who routinely used EMR systems. Construct validity was examined using Spearman's rank correlation, while internal consistency was assessed using Cronbach's alpha. Descriptive and correlational analyses were performed to examine relationships among knowledge, attitude, and behavior dimensions across seven information security focus areas.

**Results:** The instrument demonstrated acceptable item-level construct validity following item refinement and strong overall reliability. Correlation analysis revealed a patterned relationship among knowledge, attitude, and behavior, with attitude showing a stronger association with behavior than knowledge alone. Domain-level analysis further highlighted variation in awareness across focus areas, with information handling demonstrating the most pronounced behavioral gap.

**Conclusion:** The Indonesian version of the HAIS-Q provides preliminary evidence of validity and internal consistency for assessing information security awareness among medical records personnel using EMR systems. The findings emphasize the need for targeted, behavior-focused strategies to strengthen information security practices in healthcare records management contexts.

**Keywords:** information security awareness, HAIS-Q, electronic medical records, medical records personnel, knowledge, attitude, behavior

Early Version - Uncorrected

## Introduction

Electronic medical records have transformed healthcare by improving information accessibility, continuity of care, and administrative efficiency. However, this digital transformation has also increased the risk of security threats to patient data, particularly those arising from human factors. Although technical safeguards such as authentication mechanisms, access control, and

audit trails are widely implemented, healthcare data breaches continue to occur due to unsafe user behavior [1–4].

Previous studies have demonstrated that information security incidents in healthcare are frequently associated with poor password practices, failure to log out of systems, insecure use of personal devices, and inadequate incident reporting, even when organizational policies and technical protections are formally in place [3–5]. These findings indicate that safeguarding patient data requires more than technological solutions alone. Moreover, similar patterns have been reported among broader healthcare worker populations, suggesting that information handling may represent a common area of vulnerability. However, in this study, these findings are specifically observed among medical records personnel, who are directly involved in routine data management processes[6–8].

To address the human dimension of information security, a range of instruments has been developed to measure information security awareness. Nevertheless, many existing tools focus on broad constructs such as confidentiality, integrity, or access control, and often fail to capture specific behaviors that directly contribute to security vulnerabilities in practice [9]. The Human Aspects of Information Security Questionnaire (HAIS-Q) was developed to address this gap by operationalizing information security awareness through the Knowledge–Attitude–Behavior framework across seven high-risk domains, including password management, email use, mobile device use, information handling, and incident reporting [10,11]. The HAIS-Q has been validated across multiple countries and sectors and has demonstrated its ability to identify behavioral vulnerabilities that may be overlooked by technically oriented assessments [12].

Despite its relevance, the application of HAIS-Q in healthcare settings remains limited. Existing studies conducted in European contexts have adapted the instrument by reducing the number of focus areas or items, or by focusing exclusively on behavioral measures, thereby constraining its conceptual and empirical comprehensiveness [3,4]. Furthermore, to date, no formally validated Indonesian version of the HAIS-Q has been available for healthcare professionals, despite the mandatory implementation of EMR systems and the growing emphasis on patient data protection within the national health system.

Against this backdrop, the present study aimed to conduct a preliminary validation of the Indonesian version of the HAIS-Q among medical records personnel working with EMR systems in healthcare facilities. The study assessed the construct validity and internal consistency of the

Early Version - Uncorrected

instrument and examined the relationships among knowledge, attitude, and behavior dimensions of information security awareness. As a pilot validation study, the primary focus is on instrument evaluation rather than population-level inference. By providing an empirically tested measurement tool, this study seeks to support the development of targeted, human-centred interventions to strengthen patient data security practices in Indonesian healthcare settings.

## Materials and Methods

### Study Design and Setting

This study employed a cross-sectional pilot design to validate the Indonesian version of the Human Aspects of Information Security Questionnaire (HAIS-Q) and to assess information security awareness among medical records personnel using EMR systems. The study was conducted in healthcare facilities that had implemented EMR systems in accordance with Indonesia's Ministry of Health Regulation No. 24 of 2022 [13], which mandates the use of EMR in healthcare services.

### Participants and Sample Size

The study population consisted of medical records personnel who routinely used EMR systems as part of their daily work. Participants were recruited using a purposive sampling approach, targeting medical records personnel who directly interacted with electronic patient information. Inclusion criteria were active use of EMR systems and involvement in clinical or administrative workflows requiring access to patient data. Individuals without regular access to EMR were excluded.

A total of 52 medical records personnel participated in the study. This sample size was considered adequate for a pilot validation study, particularly for the assessment of item-level construct validity and the internal consistency of a multidimensional instrument. This study focused specifically on medical records personnel as the primary users of EMR systems in routine data management workflows, where they are directly involved in data entry, coding, verification, and information handling processes.

Early Version - Uncorrected

**Instrument: Indonesian Version of the HAIS-Q**

The original HAIS-Q measures information security awareness across three dimensions, knowledge, attitude, and behavior, spanning seven focus areas, including password management, email use, internet use, social media use, mobile device use, information handling, and incident reporting. The instrument comprises 63 items, with each focus area represented by three items per dimension.

The Indonesian version of the HAIS-Q was developed through a forward translation and contextual adaptation process. The initial translation was carried out by a bilingual individual with a background in health information management to ensure conceptual accuracy and domain relevance. A health information management expert subsequently reviewed the translated version to assess clarity, consistency, and contextual suitability within Indonesian healthcare settings.

Minor revisions were made to improve linguistic clarity and alignment with local terminology and routine practices related to EMR use, while preserving the original conceptual meaning of each item. Although a formal back-translation process was not conducted, the adaptation process prioritized semantic consistency and practical applicability.

All items were measured using a four-point Likert scale, with response options reflecting increasing levels of knowledge, more positive attitudes, or more secure behaviors. The absence of a neutral midpoint was intended to encourage respondents to indicate a clear tendency in their responses.

**Data Collection Procedure**

Data were collected using a self-administered questionnaire distributed to all eligible participants. Prior to data collection, participants were informed about the purpose of the study and were assured of the confidentiality and anonymity of their responses. Participation was voluntary, and completion of the questionnaire was considered as providing implied consent.

**Construct Validity Assessment**

Construct validity of the Indonesian HAIS-Q was assessed using Spearman's rank correlation to examine the relationships between individual item scores and the total scores of their

Early Version - Uncorrected

respective dimensions, knowledge, attitude, or behavior. This approach was selected due to the ordinal nature of Likert scale data.

An item was considered valid if its correlation coefficient met or exceeded 0.273 with a significance level of $p < 0.05$, corresponding to the critical value for size = 52. Items with correlation coefficients between 0.20 and 0.27 were classified as borderline and subjected to further qualitative review.

Borderline items were provisionally retained and refined through a focused group discussion with experts in medical records management and health information security. This process aimed to improve linguistic clarity, contextual relevance, and interpretability without altering the underlying construct. Items with correlation coefficients below 0.20 were excluded from the final validated item set.

### Reliability Analysis

Internal consistency of the Indonesian HAIS-Q was evaluated using Cronbach's alpha to determine the extent to which items consistently measured information security awareness as a unified construct. A Cronbach's alpha value of 0.70 or higher was considered acceptable, with higher values indicating stronger internal consistency.

### Data Analysis

Descriptive statistics were used to summarise participant characteristics and mean scores for knowledge, attitude, and behavior across the seven focus areas. Relationships among the knowledge, attitude, and behavior dimensions were examined using Spearman's rank correlation. All statistical analyses were conducted using JASP statistical software (version 0.95.4), with statistical significance set at $p < 0.05$. Given the pilot nature of the study and the relatively small sample size, advanced psychometric analyses, such as factor analysis, were not conducted.

Early Version - Uncorrected

### Ethical Considerations

The study was conducted in accordance with the ethical principles outlined in the Declaration of Helsinki. Ethical approval was obtained from the Health Research Ethics Committee of STIKES Yayasan Rumah Sakit Dr. Soetomo, Surabaya (Approval No: KEPK/XXXS/027/XX/2025). Prior to data collection, all participants received detailed information regarding the study objectives, procedures, and their rights as research subjects. Written informed consent was obtained from all participants before inclusion in the study.

Participation was voluntary, and respondents were informed of their right to withdraw from the study at any time without consequences. Data were collected anonymously and treated with strict confidentiality. Access to research data was restricted to the principal investigator and the research team, and all information was used solely for research purposes.

## RESULTS

### Construct Validity of the Indonesian HAIS-Q

As shown in Table 1, 60 of the 63 HAIS-Q items met the predefined validity criteria across the seven focus areas and three dimensions. Construct validity of the Indonesian version of the HAIS-Q was assessed using Spearman's rank correlation to examine the relationship between individual item scores and the total scores of their corresponding dimensions, namely knowledge, attitude, or behavior. This approach was selected because the data are ordinal, derived from a four-point Likert scale. Validity testing was conducted using responses from 52 medical records personnel in this study.

An item was considered to meet the validity criterion if it demonstrated a correlation coefficient of at least 0.273 with a significance level of $p < 0.05$, corresponding to the critical value for the given sample size. Items that did not meet this threshold were examined further based on the magnitude of their correlation coefficients.

The analysis showed that 60 of the 63 items met the validity requirements, indicating strong alignment between most items and their intended constructs. A small number of items yielded correlation coefficients below the statistical threshold. Items with correlation coefficients greater than 0.20 but below 0.273 were classified as borderline. These items were considered conceptually

Early Version - Uncorrected

important and potentially valid, but required refinement to improve clarity and contextual suitability.

Accordingly, borderline items were provisionally retained and subjected to linguistic and contextual refinement through a focused group discussion involving experts in medical records management and health information security. This process focused on revising item wording, simplifying sentence structure, and ensuring consistency with routine practices and policies in Indonesian healthcare settings, while preserving the original conceptual meaning of the items.

In contrast, items with correlation coefficients below 0.20 were excluded from the validated item set due to an insufficient association with their respective constructs. Such items were considered unable to adequately represent the intended dimension, even after potential linguistic adjustments.

Following this process, the Indonesian HAIS-Q retained 60 valid items, demonstrating acceptable item-level construct validity as a preliminary instrument for assessing information security awareness among medical records personnel. The presence of a small number of borderline items highlights areas where further contextual refinement may be required, particularly in domains influenced by organizational policies and patterns of technology use. Importantly, this does not compromise the instrument's overall integrity.

**Unidimensional Reliability of the Indonesian HAIS-Q**

Reliability analysis was conducted to evaluate the internal consistency of the Indonesian version of the HAIS-Q. Cronbach's alpha was used to assess the extent to which items consistently measured information security awareness as a unified construct.

The Indonesian HAIS-Q demonstrated high internal consistency. As shown in Table 2, the overall Cronbach's alpha coefficient was 0.946, with a narrow 95 per cent confidence interval, indicating a stable and reliable measurement. Item-level inspection revealed that several items exhibited negative correlations with the overall scale. These items were distributed across multiple focus areas and dimensions rather than being concentrated within a single domain.

This distribution suggests that the negative correlations did not reflect a systematic weakness in a particular construct. Instead, they may be attributable to variations in how respondents interpreted specific item wording or contextual nuances. Such patterns are not

Early Version - Uncorrected

uncommon in multidimensional instruments that assess a broad range of behaviors and attitudes related to information security.

Despite the presence of some negatively correlated items, the overall reliability of the instrument remained high. This finding supports the use of the Indonesian HAIS-Q as a consistent and dependable tool for assessing information security awareness in healthcare settings, while also identifying items that may benefit from further refinement in future validation studies.

**Correlation among Knowledge, Attitude, and Behavior (KAB)**

Spearman's rank correlation was used to examine the relationships among the knowledge, attitude, and behavior dimensions of information security awareness. The results of the correlation analysis are presented in Table 3.

A weak but statistically significant positive correlation was observed between knowledge and attitude ($r = 0.264$, $p < 0.05$), indicating that higher levels of knowledge were associated with slightly more positive attitudes towards information security. However, the strength of this association was limited.

A moderate and statistically significant positive correlation was identified between knowledge and behavior ($r = 0.400$, $p < 0.01$). This finding suggests that greater knowledge was associated with safer self-reported information security behaviors, although the magnitude of the correlation indicates that knowledge alone may not be sufficient to consistently influence behavior in routine work practices.

In contrast, a strong and statistically significant positive correlation was found between attitude and behavior ($r = 0.831$, $p < 0.01$). This result indicates that respondents with more positive attitudes towards information security were substantially more likely to report secure behaviors when using EMR systems.

Overall, the pattern of correlations demonstrates that while knowledge contributes to both attitude and behavior, attitude appears to play a more central role in translating awareness into secure practice.

Early Version - Uncorrected

**Vulnerable Areas of Information Security Awareness**

Mean scores across the seven HAIS-Q focus areas were examined to identify potential areas of vulnerability in information security awareness among electronic medical records personnel. As summarised in Table 4, awareness levels varied across the focus areas.

Knowledge scores were relatively high across most domains, including password management, email use, internet use, social media use, and incident reporting. This pattern suggests that respondents generally possessed an adequate understanding of commonly emphasized information security principles reflected in organizational policies and routine procedures.

Information handling emerged as a particularly critical area. Compared with other domains, this focus area exhibited a lower mean knowledge score, indicating gaps in respondents' understanding of appropriate practices for handling, storing, and transferring health information. In addition, information handling also demonstrated a lower mean behavior score, suggesting the inconsistent application of safe practices in daily work activities.

Notably, the mean attitude score for information handling was comparable to those observed in other domains. This pattern indicates that respondents recognised the importance of safe information handling, yet this awareness was not consistently translated into practice. The discrepancy between attitude and behavior may reflect factors such as unclear procedures, limited practical guidance, or workflow constraints that hinder the enactment of secure practices.

Other focus areas, such as mobile device use, demonstrated different patterns of vulnerability. In this domain, attitude scores were comparatively lower, while knowledge and behavior scores remained relatively high. This suggests that technical or organizational controls may support secure practices despite variations in individual attitudes.

Taken together, these findings indicate that information handling represents the most pronounced area of vulnerability among the assessed focus areas. This vulnerability appears to arise not from a lack of concern, but from gaps in practical knowledge and inconsistent behavior, underscoring the need for targeted clarification and practice-oriented guidance in this domain.

Early Version - Uncorrected

## Discussion

This study provides preliminary evidence that the Indonesian version of the HAIS-Q demonstrates acceptable item-level construct validity and internal consistency when applied to medical records personnel using medical records systems. The findings support the potential usefulness of the HAIS-Q as a tool for assessing information security awareness within this study population, where behavioral factors play a critical role in protecting patient data.

Several HAIS-Q items were excluded due to insufficient item–total correlations, particularly within the mobile device and incident reporting domains. Rather than indicating a lack of concern among medical records personnel, this pattern suggests that certain security-related behaviors may not yet be consistently internalized or clearly operationalized within routine work practices. Similar challenges have been reported in healthcare settings across low- and middle-income countries, where informal workflows, limited institutional reinforcement, and unclear accountability structures weaken adherence to formal information security behaviors [3,5].

The weak performance of items related to incident reporting warrants particular attention. Incident reporting has repeatedly been identified as one of the most vulnerable components of information security awareness in healthcare, even in organizations that have implemented formal policies and technical safeguards [4]. Organizational barriers, such as fear of blame, hierarchical reporting cultures, and the perceived low severity of security incidents, may discourage healthcare workers from reporting unsafe practices or suspected breaches. Comparable patterns have also been observed among non-clinical healthcare personnel, including medical secretaries, who are similarly involved in handling patient information within electronic health record systems. However, while medical secretaries primarily perform administrative and documentation roles, medical records personnel have more specialised responsibilities in data management and coding. Despite these differences, both roles involve direct interaction with sensitive patient data, which may explain why high levels of information security awareness do not consistently translate into secure reporting and handling practices, due to operational pressures and role-specific constraints[14].

The observed relationships among knowledge, attitude, and behavior further reinforce the theoretical foundation of the HAIS-Q instrument. Consistent with prior validation studies, higher levels of knowledge were associated with more positive attitudes towards information security, which in turn were more strongly aligned with secure self-reported behaviors [10,11]. However, the

Early Version - Uncorrected

persistence of behavioral gaps despite adequate knowledge and attitudes indicates that awareness alone is insufficient to ensure secure practices in healthcare environments. Evidence from healthcare cybersecurity research highlights the influence of contextual and organizational factors, including workload intensity, time constraints, and training practices, in shaping security behavior beyond individual awareness levels [4,12,15].

The gap between awareness and behavior may be partially explained by the habitual and routine nature of information-handling activities. When security practices are embedded within repetitive workflows, they are more likely to be enacted automatically rather than deliberately, making them vulnerable to lapses unless supported by consistent behavioral cues and organizational reinforcement [16]. Previous studies have shown that information security awareness programs are more effective when integrated into broader organizational support mechanisms than when delivered as isolated training initiatives. Evidence from health information management settings further indicates that daily workflows, role expectations, and operational demands substantially influence how staff implement information security and privacy practices during routine use of EMR [17].

From a practical perspective, these findings highlight the value of the HAIS-Q as a diagnostic tool for identifying specific behavioral vulnerabilities rather than merely measuring overall levels of awareness. The identification of low-performing focus areas, particularly information handling and incident reporting, provides actionable insight for designing targeted interventions. In healthcare settings within low- and middle-income contexts, such interventions may need to prioritise behavioral reinforcement, role-based training, and leadership engagement rather than relying solely on policy dissemination or technical controls.

This study contributes to the existing literature by extending the application of the HAIS-Q to the Indonesian healthcare context while retaining all seven focus areas of the original instrument. Unlike prior healthcare studies that reduced item coverage or focused solely on behavioral measures, this study preserves the integrated Knowledge–Attitude–Behavior framework, allowing for a more comprehensive assessment of human factors in EMR security. Although preliminary, the findings provide an initial foundation for future large-scale validation studies, including more advanced psychometric analyses such as factor analysis, and support the development of evidence-based interventions.

Early Version - Uncorrected

### Limitations of the Study

When interpreting the findings of this study, several limitations should be acknowledged. First, the study employed a cross-sectional pilot design with a relatively small sample size, which limits the generalisability of the findings beyond the specific study population of medical records personnel to other healthcare professionals or to different healthcare settings. As a result, the observed relationships between knowledge, attitude, and behavior should be interpreted as associative rather than causal.

Second, the data were collected using a self-reported questionnaire, which may introduce response bias. Participants may have overestimated their secure behaviors or responded in a socially desirable manner. Although the HAIS-Q has demonstrated strong psychometric properties, self-reported measures may not fully capture the actual information security practices as enacted in real-world healthcare environments.

Finally, this study focused on medical records personnel as the primary users of EMR systems. Consequently, the findings may not fully reflect information security awareness among other professional groups, such as clinicians, nurses, or information technology personnel, who also interact with electronic medical records in different capacities. Future research would benefit from including a broader range of professional roles and employing longitudinal designs to examine how information security awareness evolves over time, particularly as EMR systems and organizational practices continue to develop

## Conclusion

This study provides initial evidence on information security awareness among medical records personnel using EMR systems in Indonesia through the application of the Indonesian version of the Human Aspects of Information Security Questionnaire. The instrument demonstrated acceptable construct validity following item refinement and showed strong internal consistency, supporting its potential suitability as an assessment tool within healthcare records management contexts.

Early Version - Uncorrected

Analysis of the knowledge, attitude, and behavior dimensions confirms that information security awareness is a multidimensional construct. The findings further indicate that attitude is more closely aligned with secure behavior than knowledge alone. Domain-level analysis highlights information handling as the most vulnerable area, characterised by observable behavioral gaps despite relatively adequate levels of awareness.

Although exploratory in nature, these findings provide context-sensitive insights into how information security awareness is enacted in everyday healthcare records management practices. The study also establishes a foundation for future large-scale validation research and supports the development of targeted, human-centered interventions aimed at strengthening secure electronic medical record practices within healthcare organizations.

**Acknowledgment**

The authors gratefully acknowledge the support of the participating institutions and the medical records personnel who contributed their time and responses to this study.

**Funding sources**

This study was supported by a research grant from the Indonesian Association of Higher Education for Health Information Management (APTIRMIKI). The funding body had no role in the study design, data collection, data analysis, manuscript preparation, or decision to publish.

**Conflict of interest**

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Early Version - Uncorrected

**References**


1. Fernández-Alemán JL, Sánchez-Henarejos A, Toval A, Sánchez-García AB, Hernández-Hernández I, Fernandez-Luque L. Analysis of health professional security behaviors in a real clinical setting: An empirical study. International Journal of Medical Informatics. 2015 June;84(6):454–67.
2. Enaizan OM, Alwi NH, Zaizi NJ. Privacy and Security Concern for Electronic Medical Record Acceptance and Use: State of the Art. 2017;7(2).
3. Magdalinou A, Kalokairinou A, Malamateniou F, Mantas J. Assessing Internal Consistency of HAIS-Q: A Survey Conducted in Greek Hospitals. In: Mantas J, Gallos P, Zoulias E, Hasman A, Househ MS, Diomidous M, et al., editors. Studies in Health Technology and Informatics [Internet]. IOS Press; 2022 [cited 2025 Aug 2]. Available from: https://ebooks.iospress.nl/doi/10.3233/SHTI220650
4. Hore K, Hoi Tan M, Kehoe A, Beegan A, Mason S, Al Mane N, et al. Cybersecurity and critical care staff: A mixed methods study. International Journal of Medical Informatics. 2024 May;185:105412.
5. Nikbakht Nasrabadi A, Norouzkhani N, Manookian A, Cheraghi MA, Mohammadi M, Izadidastenaei Z, et al. Safeguarding Patient Information as an Issue Faced by Nurses: A policy brief. APJHM [Internet]. 2024 July 23 [cited 2025 Aug 10]; Available from: https://journal.achsm.org.au/index.php/achsm/article/view/3013
6. Sari PK, Handayani PW, Hidayanto AN. Demographic Comparison of Information Security Behavior Toward Health Information System Protection: Survey Study. JMIR Form Res. 2023 Aug 24;7:e49439.
7. Sari PK, Sutanto J, Handayani PW, Hidayanto AN. Information Security Behavior of Healthcare Professionals when There is Poor Health Information Security Policy. 2024;
8. Sari PK, Trianasari N, Prasetio A. Investigating the Main Factors Affecting Healthcare Workers' Information Security Behaviors: An Empirical Study in Indonesia. JISIS. 2025 Feb 28;15(1):1–15.
9. Gebeyew AS, Wordofa ZR, Muluneh AA, Shibabaw AA, Walle AD, Tizie SB, et al. Attitudes of Health Professionals Toward Digital Health Data Security in Northwest


Early Version - Uncorrected

Ethiopia: Cross-Sectional Study. Online J Public Health Inform. 2024 Nov 6;16:e57764–e57764.

10. Parsons K, McCormac A, Butavicius M, Pattinson M, Jerram C. Determining employee awareness using the human aspects of information security questionnaire (HAIS-Q). Computers & security. 2014;42:165–76.
11. Parsons K, Calic D, Pattinson M, Butavicius M, McCormac A, Zwaans T. The Human Aspects of Information Security Questionnaire (HAIS-Q): Two further validation studies. Computers & Security. 2017 May 1;66:40–51.
12. Fujs D, Vrhovec S, Vavpotic D. Know Your Enemy: User Segmentation Based on Human Aspects of Information Security. IEEE Access. 2021;9:157306–15.
13. Hossain MdK, Sutanto J, Handayani PW, Haryanto AA, Bhowmik J, Frings-Hessami V. An exploratory study of electronic medical record implementation and recordkeeping culture: the case of hospitals in Indonesia. BMC Health Serv Res. 2025 Feb 14;25(1):249.
14. Filik T, Ünalan D. The evaluation of the effect of the information security awareness level in medical secretaries on the security and privacy implementations of electronic health records. Hacettepe Sağlık İdaresi Dergisi [Internet]. 2021;(Query date: 2025-05-15 22:30:54). Available from: https://dergipark.org.tr/en/pub/hacettepesid/issue/60872/902620
15. Nifakos S, Chandramouli K, Nikolaou CK, Papachristou P, Koch S, Panaousis E, et al. Influence of Human Factors on Cyber Security within Healthcare Organisations: A Systematic Review. Sensors. 2021 July 28;21(15):5119.
16. Sher ML, Talley PC, Cheng TJ, Kuo KM. How can hospitals better protect the privacy of electronic medical records? Perspectives from staff members of health information management departments. HIM J. 2017 May;46(2):87–95.
17. Kim Y. Awareness of, attitudes towards, and practices of health information management professionals in South Korea relating to privacy of personal health information. HIM J. 2023 Jan 1;52(1):50–6.

Early Version - Uncorrected

**Table 1.** Summary of Item Validity of the Indonesian HAIS-Q by Focus Area and Dimension

| Focus Area | Dimension | Total Items | Valid Items (n) | Invalid Items (n) | Percentage Valid |
|---|---|---|---|---|---|
| Password Management | Knowledge | 3 | 3 | 0 | 100% |
| | Attitude | 3 | 3 | 0 | 100% |
| | Behavior | 3 | 3 | 0 | 100% |
| Email | Knowledge | 3 | 3 | 0 | 100% |
| | Attitude | 3 | 3 | 0 | 100% |
| | Behavior | 3 | 3 | 0 | 100% |
| Internet | Knowledge | 3 | 3 | 0 | 100% |
| | Attitude | 3 | 3 | 0 | 100% |
| | Behavior | 3 | 3 | 0 | 100% |
| Social Media | Knowledge | 3 | 3 | 0 | 100% |
| | Attitude | 3 | 2 | 1 | 66.7% |
| | Behavior | 3 | 3 | 0 | 100% |
| Mobile Devices | Knowledge | 3 | 2 | 1 | 66.7% |
| | Attitude | 3 | 3 | 0 | 100% |
| | Behavior | 3 | 2 | 1 | 66.7% |
| Information Handling | Knowledge | 3 | 3 | 0 | 100% |
| | Attitude | 3 | 3 | 0 | 100% |
| | Behavior | 3 | 3 | 0 | 100% |
| Incident Reporting | Knowledge | 3 | 3 | 0 | 100% |
| | Attitude | 3 | 3 | 0 | 100% |
| | Behavior | 3 | 3 | 0 | 100% |
| **Total** | | **63** | **60** | **3** | **95%** |

Note: Item validity was assessed using Spearman's rank correlation ($r \geq 0.273$, $p < 0.05$). Items with correlation coefficients between 0.20 and 0.27 were reviewed and refined through focused group discussion (FGD), while items with coefficients below 0.20 were excluded from the validated item set.

Early Version - Uncorrected

**Table 2.** Reliability Analysis of the Indonesian HAIS-Q

| Coefficient | Estimate | Standard Error | 95% CI (Lower) | 95% CI (Upper) |
|---|---|---|---|---|
| Cronbach's alpha | 0.946 | 0.013 | 0.921 | 0.971 |

**Table 3.** Correlations among Knowledge, Attitude, and Behavior

| Variabel | Knowledge | Attitude | Behavior |
|---|---|---|---|
| Knowledge | 1.000 | 0.264* | 0.400** |
| Attitude | 0.264* | 1.000 | 0.831** |
| Behavior | 0.400** | 0.831** | 1.000 |

Note: * $p < 0.05$; ** $p < 0.01$ (Spearman's rank correlation).

**Table 4.** Mean Knowledge, Attitude, and Behavior Scores across the Seven Focus Areas

| Focus Area | Mean Level of Knowledge | Mean Level of Attitude | Mean Level of Behavior |
|---|---|---|---|
| Password Management | 10,79 | 8,29 | 8,81 |
| Email Use | 10,37 | 7,96 | 7,98 |
| Internet Use | 10,83 | 7,02 | 8,42 |
| Mobile Device | 10,29 | 4,65 | 10,10 |
| Information Handling | 6,69 | 7,92 | 5,19 |
| Social Media use | 10,58 | 7,62 | 8,02 |
| Incident Reporting | 10,31 | 7,65 | 9,15 |

Note: Scores were calculated based on three items per dimension using a four-point Likert scale (range: 3–12). Higher scores indicate higher levels of knowledge, more positive attitudes, or more secure behaviors.

Early Version - Uncorrected