Received: 6 August 2021 | Revised: 24 March 2022 | Accepted: 22 August 2022

DOI: 10.1002/nop2.1353

RESEARCH ARTICLE

NursingOpen Open Access WILEY

Development and validation of the information security attitude questionnaire (ISA-Q) for nurses

Jiwon Kang[1] | GyeongAe Seomun[2]

[1]School of Nursing, University of Minnesota, Minneapolis, Minnesota, USA

[2]College of Nursing, BK21FOUR R&E Center for Learning Health Systems, Korea University, Seoul, Republic of Korea

Correspondence
GyeongAe Seomun, College of Nursing, Korea University, 145, Anam-ro, Seongbuk-gu, Seoul, Republic of Korea.
Email: seomun@korea.ac.kr

Funding information
Korea University Nursing Research Institute, Grant/Award Number: 2022

Abstract

Aim: The aim of the study was to understand nurses' information security attitudes towards patient information. This study developed the Information Security Attitude Questionnaire (ISA-Q) to measure the physical, technical and administrative aspects of information security for nurses and assessed its validity and reliability.

Design: Cross-sectional study and scale development.

Methods: Exploratory and confirmatory factor analyses and correlation analyses were performed to assess construct, discriminant and convergent validity; Cronbach's α and test–retest reliability were examined.

Results: Exploratory and confirmatory factor analyses yielded a 6-factor, 30-item solution. Six factors accounted for 60.19% of the total variance. The confirmatory factor analysis was achieved through structural equation modelling. Discriminant and convergent validity were confirmed. The internal consistency of the ISA-Q was 0.94, and the test–retest reliability was 0.74. The ISA-Q is an appropriate questionnaire for identifying information security attitudes of nurses, making it useful for developing systematic performance methods to enhance nurses' information security levels.

KEYWORDS
administrative, information security, physical, questionnaire development, technical

1 | INTRODUCTION

The provision of nursing services has undergone several changes with the development of information and communication technologies (Oh, 2015; Rouleau et al., 2017). In such a rapidly changing healthcare environment, the importance of securing patients' clinical information related to the provision and maintenance of high-quality nursing services is increasing (Smaradottir, 2017). Statistics show that there were 3,705 medical data breaches between 2009–2020, including more than 500 records, which damaged more than 2.6 billion medical records, accounting for nearly 81.72% of the US population (HIPAA Journal, 2021). Most breaches are caused by human error (Algarni et al., 2018) and can occur when nurses or clinicians accidentally share confidential information in a conversation, or when a file containing confidential information is lost or carelessly discarded (van der Wens, 2019). Therefore, nurses who communicate closely with patients should take the necessary security measures to protect patient data and recognize the importance of patient clinical information (Kim, 2012).

Attitude is an important predictor of behaviour (Kim & Hunter, 1993a, 1993b) and plays an important role in protecting electronic health records security and patient privacy for nurses. A nurse's information security attitude can be used as a basic guideline

for protecting a patient's private health information and can also help develop the nursing information security programme and curricula in the future.

2 | BACKGROUND

Information security means processes and methodologies designed to protect confidential, personal and sensitive information or data from unauthorized access, use, misuse, public destruction, modification or disruption of information (SANS Institute, 2021). Attitude, which is the most important factor influencing nurse's information security behaviour, acts as an important variable to be supported, especially for the behaviour to secure patients' clinical information (Ajzen, 1991; Kang & Seomun, 2021). Since the nurse acts as a key person in handling patient information (Hartigan et al., 2018), the nurse's attitude to handling patient information is most important and the nurse needs to recognize the importance of patient information security (Jung & Jung, 2014).

Despite the increased risk of external exposure of patients' clinical information, the information security attitudes of nurses remain at the conceptual exploration level (Kang & Seomun, 2021). Existing questionnaires do not integrate and reflect all physical, technical and administrative aspects of information security (Andriole, 2014), but mainly consist of questions related to the administrative and physical aspects (Bulgurcu et al., 2010; Parsons et al., 2017; Velki et al., 2014). To view and measure the information security attitude of nurses in an integrated view, information security attitudes of nurses should include the physical security aspects as a means of protecting information from trespassing and environmental hazards; technical security aspects serving to access, authenticate and control patients' clinical information; and administrative security aspects about procedures, policies and training (Kang & Seomun, 2021; Kruse et al., 2017).

2.1 | Aims

This study aimed to develop a questionnaire with high validity and reliability that comprehensively deals with the physical, technical, and administrative aspects of information security to measure nurses' attitudes towards information security. Based on this result, it will be possible to support the development of a progressive education programme on clinical information security for nurses and to evaluate its effectiveness.

3 | THE STUDY

3.1 | Design

The study participants were selected from the general ward, emergency room, intensive care unit and outpatient nurses based on their agreement with the study purpose. The sample size should be 10 or more per item (Everitt, 1975), and the number of samples required for analysis should be at least 300 (Lee et al., 2009). Hence, a cross-sectional study was conducted with 445 nurses, and 372 copies (valid response rate = 83.6%) were included in the final analysis.

3.2 | Method

The development and validation of the ISA-Q was conducted as per the eight steps of scale development and verification (DeVellis, 2016).

3.2.1 | Components of the questionnaire

Prior to the production of the questionnaire, important elements derived from conceptual analysis (Kang & Seomun, 2021) were used to establish the components of the ISA-Q. Through three elements of physical, technical and administrative domains of information security, seven attributes (i.e. environmental control, facility stability, information accessibility, taking advantage of features, systematicity of work, execution of education and professional responsibility) for information security in nursing were identified in the concept analysis (Kang & Seomun, 2021) and used to construct the questionnaire contents. From this, preliminary items were formed as empirical indicators, followed by a content validity process.

3.2.2 | Writing the items

Using the above procedure, 36 preliminary questions were listed. To improve readability, multiple meanings were avoided, and one question was omitted due to its applicability to various situations (DeVellis, 2016).

3.2.3 | Determining the questionnaire

Regarding the questionnaire's scoring method, a five-point Likert questionnaire was dismissed as it was likely to cause people to maintain a neutral position, thereby decreasing the reliability of responses (Kim & Shin, 2016; Lee et al., 2009). Hence, a four-point Likert scale was used. A higher score indicates a higher level of information security attitude.

3.2.4 | Expert content validity test

Ten experts participated for the content validation of the ISA-Q factors and items (Lynn, 1986). We formed a specialist group consisting of four nursing managers, four nurses with more than 20 years of clinical experience, and two patients' clinical information security experts to test the content validity of the questionnaire's components

and items. We calculated the validity of each item using the following scoring method: highly agree = 4, agree = 3, disagree = 2 and highly disagree = 1. We deleted items with a calculated value of 80% or less.

3.2.5 | Item review

A preliminary survey with six nurses was undertaken and the questionnaire revised. We shortened all lengthy sentences to improve clarity and removed all unnecessary or ambiguous words to ensure a sufficient transfer of meaning (DeVellis, 2016).

3.2.6 | Administering the items

We collected data using the final questionnaire after obtaining permission from the health institutions. Information was provided about the research objectives and anonymity and participants submitted a consent form before the survey began. Each completed questionnaire was sealed in an envelope and collected directly by the researchers to ensure the anonymity of the responses.

3.2.7 | Evaluating the items

Evaluation of construct validity

The collected data were analysed using Kaiser-Meyer-Olkin (KMO) measurement and Bartlett's sphere formation test. This analysis determined whether the preliminary items were suitable for exploratory factor analysis (EFA; Fabrigar & Wegener, 2011). We used principal component analysis (PCA) for varimax rotation. To ensure the best fit for the analysis model, we employed the varimax method. It is an orthogonal factor rotation method used when the correlation between factors is not assumed (Kaiser, 1958). This method assumes that the correlation between the factors is 0 and can facilitate factor structure analysis (Fabrigar & Wegener, 2011). We extracted relevant factors from the PCA using items with an eigenvalue of 1.0 or higher and a factor loading of 0.40 or higher (Bobko & Schemmer, 1984; Fabrigar & Wegener, 2011). Confirmatory factor analysis (CFA) was achieved through structural equation modelling. We used maximum likelihood estimation as the estimation method and combined the absolute and incremental fit indices to measure fitness. After the model fit test, intensive validity was examined using average variance extracted (AVE) and construct reliability (CR). If the AVE is 0.50 or more and the CR is 0.70 or more, it has appropriate intrinsic validity (Woo, 2016).

Evaluation of discriminant validity

The instrument was tested for validity using discriminant validity. If the variance extraction index between the two factors was higher than the square of the correlation coefficient of each (that is, the co-efficient of determination) their discriminant validity was confirmed (Woo, 2016).

Evaluation of convergent validity

We analysed the convergent validity of the ISA-Q by analysing the correlation between ISA-Q, the Human Information Security Questionnaire (HAIS-Q; Velki et al., 2014) and the correlation between ISA-Q and Patient Privacy Protection Behaviour Awareness and Practice (Lee & Park, 2005).

Evaluation of reliability

Cronbach's alpha and Pearson's correlations were calculated to test the reliability of the instrument. The test–retest reliability was based on the first questionnaire completed by the participants and the questionnaire administered 2 weeks later. This confirmed the stability of the correlation. Retesting is appropriate after 2–4 weeks when the subject's memory of the first test is limited (Lee et al., 2009).

3.2.8 | Questionnaire optimization

The items of the final questionnaire were confirmed according to the validity and reliability tests.

3.3 | Ethics

This study was approved by the Institutional Review Board of Korea University (1040548-KU-IRB-17-131-A-2) prior to data collection. Additionally, we collected data from only those participants who understood the purpose of the study and agreed to participate voluntarily.

4 | RESULTS

4.1 | Development of the ISA-Q

4.1.1 | Identification of the ISA-Q

The primary version of the ISA-Q comprised 36 items. A four-point questionnaire was used to rate information security attitude levels, ranging from 1 (not at all) to 4 (very agreeable); a higher score indicates a higher level of information security attitude.

4.1.2 | Content validity

Three items were suggested for removal by the experts. Their items and attributes were as follows: “I always check to see if anyone is unrelated to my care when I record my nursing information”—“Environmental control”; “I collect patient information where it is unlikely that patient information will be leaked”—“Environmental control”; and “I use the program that records medical information comfortably.”—“Take advantage of features.” The Content Validity

Index (CVI) of the remaining 33 items was higher than 0.8, with an average CVI of 0.97, indicating that the remaining items did not require additional revisions.

4.2 | Psychometric analysis of the ISA-Q

4.2.1 | Respondent characteristics

A total of 372 surveys were analysed. The participants' general characteristics are presented in Table 1.

4.2.2 | Item analysis

After analysing the mean, standard deviation, skewness and kurtosis of each item, two items with skewness and kurtosis exceeding the reference value were deleted. The 31 items revealed item–total correlation coefficients of >0.40. Content analysis, conducted by calculating the corrected item–total correlation coefficients and the coefficients of the items, showed a correlation distribution from 0.445–0.722.

4.2.3 | Construct validity

Exploratory factor analysis

Exploratory factor analysis was carried out for the 31 items selected by content analysis. In this study, EFA was performed on 30 items; one item with a commonality value of <0.40 (0.397) was excluded. For the final 30 items, the KMO measure of sampling adequacy was high (0.93), and Bartlett's test of sphericity showed a significant p-value ($\chi^2 = 5{,}434.900$, $p < .001$). Both indicate that the data are appropriate for EFA. The results of EFA revealed that the eigenvalues of the six factors were more than 1 and met the Kaiser's criteria. The results are presented in Table 2.

The seven factors in Kang and Seomun's (2021) conceptual analysis were converted into six concepts after EFA analysis, according to their factor loadings, and renamed as follows: "Information accessibility" to "Restricting access to information (four items)," "Environmental control" remained "Environmental control (three items)," "Facility stability" to "Maintaining facility stability (four items)" (after the EFA analysis, "Take advantage of features" converged with "Facility stability" and the final name of "Maintaining facility stability" was obtained), "Systematicity of work" to "Work systematicity (nine items)," "Exclusion of education" to "Continuous education participation (five items)" and "Professional responsibility" to "Promoting professional responsibility (five items)." In this study, the correlation coefficient between factors was <0.85; thus each factor was interpreted as having a characteristic and discriminant power.

Confirmatory factor analysis

According to the factor structure identified using EFA, CFA was then used to test the goodness of fit of the model structure. The six-factor model composed of 30 items had an acceptable fit (root mean square error of approximation [RMSEA] = 0.064, root mean square residual [RMR] = 0.022, comparative fit index [CFI] = 0.89, adjusted goodness of fit index [AGFI] = 0.82, normed fit index [NFI] = 0.82). The final model of ISA-Q is presented in Figure 1. As a result of the model fit test, the ISA-Q was deemed to have conformity. The CR of the questionnaire was 0.755–0.956, which met the criterion of 0.7 or higher. The AVE ranged from 0.509–0.792, as shown in Table 3. Based on these results, it could be considered to have appropriate intensive validity.

TABLE 1 General characteristics of study participants ($N = 372$)

Variable	Category	N	(%)	Mean ± SD
Sex	Male	10	2.7	
	Female	362	97.3	
Age				31.3 ± 6.9
Marital status	Married	138	37.1	
	Single	234	62.9	
Education	3-year graduation	89	23.9	
	4-year graduation	213	57.3	
	Graduate school or higher	70	18.8	
Position	Chief nurse	9	2.4	
	Charge nurse	250	67.2	
	Nurse	113	30.4	
Department	Ward	180	48.4	
	Outpatient	109	29.3	
	Special	83	22.3	
Total clinical work experience (year)				8.6 ± 7.1
Current department work experience (year)				5.2 ± 4.5

TABLE 2 Exploratory factor analysis of the ISA-Q

Factor	Items	Factor loadings					
		1	2	3	4	5	6
Work systematicity	21. I follow the reporting and processing procedures in case of accidental patient information leakage.	0.708	0.196	0.329	0.126	0.135	0.105
	18. I carry out nursing work according to the medical institution's information security policy and system.	0.674	0.316	0.090	0.069	0.179	0.207
	23. I am aware of natural disasters and emergency measures/ procedures.	0.652	0.030	0.463	0.162	−0.037	0.240
	17. I identify and observe the medical institution's policies for information security.	0.647	0.308	0.076	0.131	0.170	0.134
	19. I follow the management protocol for patients' clinical information storage needs (external hard dis, USB, etc.).	0.616	0.093	0.121	0.363	0.264	0.001
	20. I follow the prescribed procedure when reading special information, such as the patient's psychiatric information.	0.611	0.266	0.195	0.061	0.340	0.123
	22. I immediately report any vulnerability to patients' clinical information security.	0.563	0.091	0.265	0.356	−0.044	0.175
	16. I facilitate communication with the computer security team in the event of a security issue.	0.537	0.290	0.112	0.378	0.224	−0.101
	9. I am aware of the location and use of firefighting equipment installed as preparedness for disasters.	0.457	0.104	0.185	0.060	0.239	0.313
Promoting professional responsibility	31. I do not share patients' clinical information without their consent.	0.235	0.755	0.182	0.082	0.059	0.066
	30. When I share patients' clinical information on the job, I only expose the relevant contents to the concerned person.	0.212	0.735	0.207	0.160	0.071	0.256
	29. I do not reveal patients' clinical information in a private setting.	0.137	0.694	0.233	0.184	0.008	0.310
	32. I treat clinical information of patients, who apply for restriction of medical information, separately.	0.206	0.667	0.280	0.136	0.185	−0.028
	33. I do not look up patients' clinical information unless for the job.	0.189	0.606	0.249	0.047	0.201	0.212
Continuous education participation	25. I am familiar with the legal responsibilities of nursing records.	0.174	0.268	0.754	0.177	0.214	0.031
	26. I am trained in using patients' clinical information-related programmes.	0.107	0.248	0.689	0.105	0.287	0.117
	28. I have received employee emergency training for natural disasters and other disasters.	0.253	0.167	0.678	0.194	−0.050	0.145
	24. I learn about the importance of patients' clinical information security through nurse position training.	0.184	0.262	0.676	0.162	0.143	0.132
	27. I identify and train the security status of successor nurses (or nursing students).	0.244	0.270	0.512	0.173	0.086	0.204

TABLE 2 (Continued)

Factor	Items	Factor loadings					
		1	2	3	4	5	6
Maintaining facility stability	5. I make sure the notation is encrypted when the patient's unique information is output.	0.142	0.078	0.320	0.722	0.051	0.134
	4. I make sure the screen saver is active when I leave.	0.169	0.116	0.235	0.657	0.052	0.267
	7. I confirm that the healthcare information system always remains available.	0.277	0.320	0.051	0.562	0.250	0.091
	8. I ensure a stable supply of power to medical equipment and computer-related equipment.	0.258	0.131	0.102	0.471	0.149	0.220
Restricting access to information	14. It is desirable that the authority for reading patients' clinical information is applied according to my rank (or the department).	0.133	0.056	0.170	0.219	0.726	0.093
	12. It is desirable that the right to access information be modified following my work status change (personnel transfer, retirement, etc.).	0.195	0.155	0.146	0.130	0.701	0.263
	15. My medical information system access record should preferably be archived.	0.470	0.141	0.016	0.184	0.579	−0.069
	11. I change my password for business use regularly.	0.216	0.136	0.171	−0.212	0.490	0.357
Environmental control	2. I keep the printouts containing patients' clinical information strictly in the designated area.	0.177	0.222	0.013	0.189	0.143	0.687
	10. I do not use others' ID and password when accessing patient clinical information systems.	0.126	0.194	0.217	0.113	0.057	0.601
	3. I destroy prints related to patient clinical information when there is no use for them at work.	0.070	0.074	0.175	0.335	0.181	0.594
	Eigenvalue	4.328	3.421	3.327	2.491	2.357	2.133
	Variance explained (%)	14.427	11.402	11.090	8.302	7.858	7.110
	Cumulative variance explained (%)	14.427	25.829	36.919	45.221	53.079	60.189

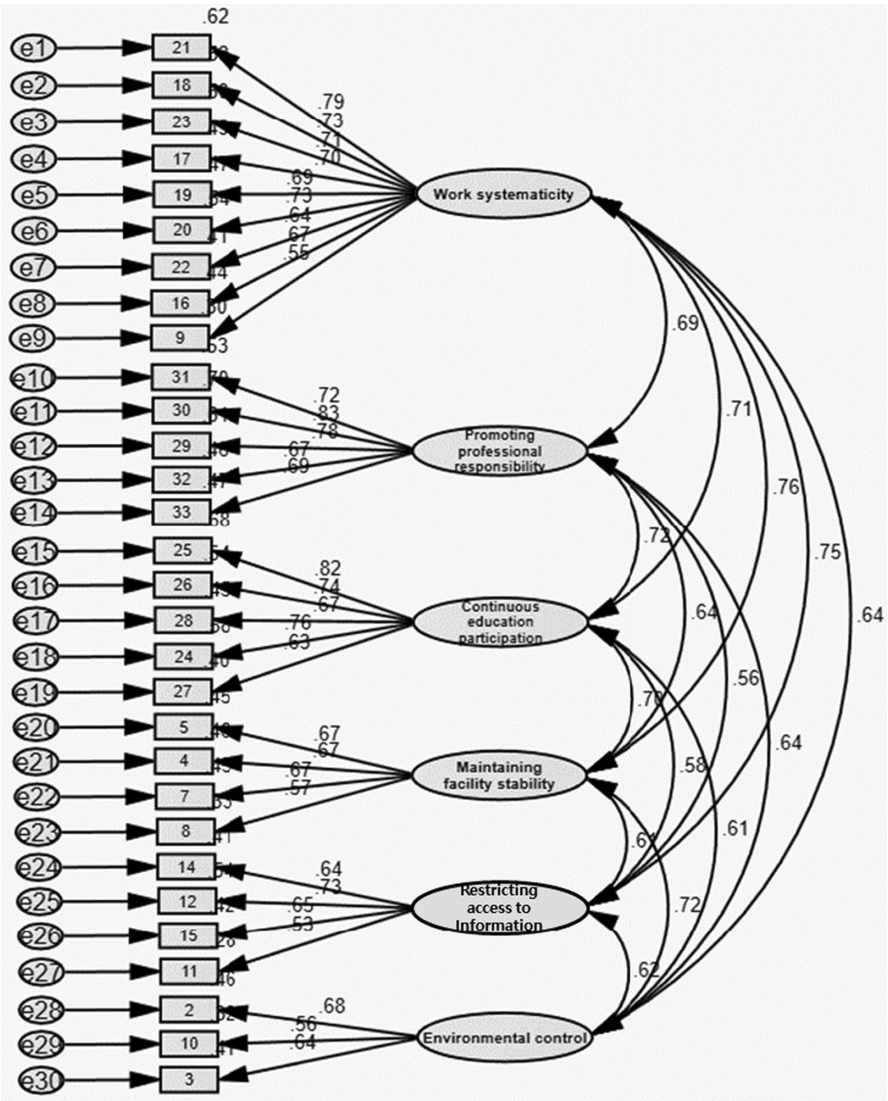

FIGURE 1 Model for confirmatory factor analysis of the ISA-Q

4.2.4 | Discriminant validity

The variance extraction index of the model was confirmed to be greater than the value of all the determinants (the square of the correlation), confirming that discriminant validity was secured, as shown in Table 4.

4.2.5 | Convergent validity

We calculated correlations between the ISA-Q and HAIS-Q, and the ISA-Q and Patient Privacy Protection Behaviour Awareness and Practice to verify convergent validity. Table 5 shows the convergent validity of ISA-Q. The correlation coefficient of ISA-Q and HAIS-Q was 0.63, and a statistically significant net correlation appeared for all six factors. The correlation coefficient of ISA-Q, Patient Privacy Protection Behaviour Awareness and Practice was 0.63; a statistically significant net correlation appeared for all six factors.

4.2.6 | Reliability

The internal consistency reliability of Cronbach's α value for the questionnaire was .94. In each factor, Cronbach's α value was .89 for work systematicity, .86 for promoting professional responsibility, .84 for continuous education participation, .74 for maintaining facility stability, .73 for restricting access to information, and .64 for environmental control. The ISA-Q was repeatedly administered to 181 participants to examine the test–retest reliability, and 73 participants were included in the final analysis. The coefficient for ISA-Q was found to be 0.74. Therefore, it can be considered a stable and reliable questionnaire because the test–retest correlation coefficient is above 0.70 (DeVon et al., 2007).

5 | DISCUSSION

This study developed the ISA-Q to measure the nurses' attitudes regarding the physical, technical and administrative aspects of

TABLE 3 Intensive validity of the ISA-Q ($N = 372$)

Factor	Item	Factor loading	Error	AVE	CR
Work systematicity	21	0.790	0.162	0.625	0.956
	18	0.729	0.152		
	23	0.707	0.248		
	17	0.701	0.199		
	19	0.688	0.292		
	20	0.734	0.182		
	22	0.644	0.348		
	16	0.666	0.253		
	9	0.547	0.278		
Promoting professional responsibility	31	0.725	0.135	0.792	0.950
	30	0.835	0.088		
	29	0.782	0.126		
	32	0.675	0.199		
	33	0.687	0.189		
Continuous education participation	25	0.824	0.128	0.729	0.931
	26	0.738	0.182		
	28	0.672	0.260		
	24	0.761	0.138		
	27	0.632	0.297		
Maintaining facility stability	5	0.671	0.399	0.718	0.910
	4	0.675	0.288		
	7	0.672	0.205		
	8	0.572	0.387		
Restricting access to information	14	0.642	0.266	0.631	0.871
	12	0.732	0.166		
	15	0.647	0.194		
	11	0.525	0.284		
Environmental control	2	0.682	0.141	0.509	0.755
	10	0.562	0.340		
	3	0.643	0.291		

TABLE 4 Discriminatory validity for the ISA-Q

	Factor 1	Factor 2	Factor 3	Factor 4	Factor 5	Factor 6
Factor 1	**0.791**[a]					
Factor 2	0.688 $p < .001$	**0.890**[a]				
Factor 3	0.714 $p < .001$	0.718 $p < .001$	**0.854**[a]			
Factor 4	0.758 $p < .001$	0.638 $p < .001$	0.696 $p < .001$	**0.847**[a]		
Factor 5	0.751 $p < .001$	0.557 $p < .001$	0.582 $p < .001$	0.615 $p < .001$	**0.794**[a]	
Factor 6	0.637 $p < .001$	0.637 $p < .001$	0.608 $p < .001$	0.717 $p < .001$	0.616 $p < .001$	**0.713**[a]

[a]The diagonal bold value is the square root of AVE.

patients' information security. These constructed questions were based on a conceptual analysis (Kang & Seomun, 2021) not utilized by existing questionnaires. The ISA-Q consists of six factors and 30 items on three aspects of security: administrative (work systematicity, promoting professional responsibility and continuous education participation), physical (maintaining facility stability and environmental control) and technical (restricting access to information). The psychometric verification process confirmed the reliability

TABLE 5 Convergent validity for the ISA-Q ($N = 372$)

	ISA-Q	HAIS-Q		Patient privacy protection behaviour awareness and practice	
	Mean ± SD (min-max; 1–4)	Mean ± SD (min-max; 31–105)	*r*	Mean ± SD (min-max; 39–195)	*r*
Total ISA-Q	3.43 ± 0.40 (2–4)	91.58 ± 10.61 (53–107)	.63**	170.96 ± 19.37 (107–195)	.63**
Factor 1	3.37 ± 0.49 (2–4)		.55**		.56**
Factor 2	3.56 ± 0.45 (2–4)		.53**		.62**
Factor 3	3.41 ± 0.51 (2–4)		.51**		.53**
Factor 4	3.26 ± 0.56 (2–4)		.49**		.42**
Factor 5	3.51 ± 0.46 (2–4)		.42**		.41**
Factor 6	3.51 ± 0.49 (2–4)		.43**		.42**

**$p < .01$.

and validity of the questionnaire for measuring nurses' information security attitudes in various situations.

In this study, "work systematicity" was the first factor in the administrative aspect of information security. It emphasizes that systems and operational processes for information management should be actively constructed and utilized as a foolproof device (MacMillan, 2021; O'Brien & Marakas, 2006). It recognizes that nurses need to manage information on a system and the importance of maintaining protocols. "Promoting professional responsibility" was devised as the second factor in the administrative aspect of information security. This implies that it is essential to strengthen the sense of responsibility as a professional nurse in the practice of patients' clinical information security activities. Such an attitude gains a patient's trust and creates satisfactory nursing results. Protecting and securing personal information is an important responsibility of a nurse and plays a role in protecting the self-esteem of patients and advocating for their rights (Mannix et al., 2015). The third factor in the administrative aspect of information security was "participation in continuous education." Previous studies on health professionals' attitudes towards information security have emphasized the necessity of continuous education (Kim et al., 2013; Mannix et al., 2015). While it is important to create educational opportunities to help nurses create new knowledge, it is also necessary to encourage evidence-based methods, such as action plans and participatory approaches, to help nurses participate in education (Kinnunen et al., 2022). The importance of continuing education for nurses is always emphasized; however, if the need for nurses is not felt and not motivated, the value of education will be underestimated. Hence, a plan for a user-centred work environment, motivation and social support should be established to reinforce the use of trained information security competencies (Virtanen et al., 2021).

"Maintaining the stability of a facility" was devised as the first factor in the physical aspect of information security. The importance of the stability of building structures and working environments in preparation for natural or security disasters has previously been discussed (Kim, 2012; MacMillan, 2021). A nurse needs to monitor the condition of the facility and keep it operational to ensure its stability. "Environmental control" emerged as the second most important factor in the physical aspect of information security. The information system and equipment of an institution should be kept safe from intrusion (Chung et al., 2012). Actions such as leaving nurse workstations in an unsecured state or improperly organizing or disposing documents can be unintentional; these actions raise serious concerns about the safety and protection of patient information. According to Blanke and McGrady (2016), portable device breaches were the highest among the reported threats, and loss and theft, such as of mobile devices, contributed to cyber threats. Nurses must emphasize and recognize that patient information should be handled in a manner that prevents direct exposure in case of an information threat inside or outside the work environment.

Finally, restricting information accessibility was the primary factor in the technical aspect of information security. Nurses should collect patient information for therapeutic purposes, and not identify a patient's sensitive information or use other personal information without the patient's consent in a multidisciplinary approach (Chung et al., 2012). From a technical point of view, an organization should establish a security architecture to restrict access to information by classifying the use of personal or sensitive information of patients by medical staff.

The ISA-Q was developed to overcome the limitations of existing questionnaires. The ISA-Q can be administered with validity and reliability in nursing practice and research. Additionally, it can provide data on human resource management for preparing educational programmes and harmonizing hospital organizations. The ISA-Q can also be considered as an effective intervention strategy for nurse management by accessing information security and developing security intervention programmes. Finally, it allows for the identification and understanding of information security in clinical nursing practice, as well as its various levels. Thus, nurses can develop a systematic method to enhance and utilize patients' clinical information.

5.1 | Limitations

The ISA-Q was found to be an appropriate questionnaire for identifying attitudes based on the perception of nurses' information security; however, it is necessary to distribute the questions by each factor. A deeper interpretation of the components

is required to understand nurses' attitudes towards information security in detail, and related research should be continued. The validity and reliability of the ISA-Q should be re-evaluated for nurses in various workplaces. In addition, since the ISA-Q does not select the number of questions according to the importance of each factor, this aspect should be compensated for during the refinement process.

6 | CONCLUSION

In this study, we developed the ISA-Q and verified its validity and reliability. This questionnaire consisted of six factors that measure the information security attitude of nurses by integrating the physical, technical and administrative aspects of information security. The instrument was tested for construct, discriminant and convergent validity and reliability. Its explanatory power was analysed as 60.19%.

This questionnaire can be used to identify the status of nurses' information security attitudes and to further research into the development and application of nursing interventions and education programmes that can enhance them.

AUTHOR CONTRIBUTION

JK and GS designed the study, supervised the study, wrote the manuscript and critically revised the study for important intellectual content. JK collected the data and analysed the data.

ACKNOWLEDGEMENT

We would like to thank the participants of this study.

FUNDING INFORMATION

This work was supported by grants from Korea University Nursing Research Institute; 2022.

CONFLICT OF INTEREST

The authors declare that there is no conflict of interest.

DATA AVAILABILITY STATEMENT

The data that support the findings of this study are available from the corresponding author upon reasonable request.

ETHICAL APPROVAL

This study obtained ethical approval from the institutional review board of Korea University (1040548-KU-IRB-17-131-A-2).

ORCID

Jiwon Kang https://orcid.org/0000-0002-7272-0360
GyeongAe Seomun https://orcid.org/0000-0002-1651-5741

REFERENCES

Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes*, *50*(2), 179–211. https://doi.org/10.1016/0749-5978(91)90020-T

Algarni, M., Almesalm, S., & Syed, M. (2018). Towards enhanced comprehension of human errors in cybersecurity attacks. In R. L. Boring (Ed.), *Advances in intelligent systems and computing* (pp. 163–175). Springer. Paper presented at the International Conference on Applied Human Factors and Ergonomics, Cham.

Andriole, K. P. (2014). Security of electronic medical information and patient privacy: What you need to know. *Journal of the American College of Radiology*, *11*(12), 1212–1216. https://doi.org/10.1016/j.jacr.2014.09.011

Blanke, S. J., & McGrady, E. (2016). When it comes to securing patient health information from breaches, your best medicine is a dose of prevention: A cybersecurity risk assessment checklist. *Journal of Healthcare Risk Management*, *36*(1), 14–24. https://doi.org/10.1002/jhrm.21230

Bobko, P., & Schemmer, F. M. (1984). Eigenvalue shrinkage in principal components based factor analysis. *Applied Psychological Measurement*, *8*(4), 439–451. https://doi.org/10.1177/014662168400800408

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

Chung, K.-I., Park, H.-A., Jung, B.-G., Jang, J.-S., & Chung, M.-A. (2012). Big data and information security. *Journal of Advanced Information Technology and Convergence (JAITC)*, *10*(3), 17–22.

DeVellis, R. F. (2016). *Questionnaire development: Theory and applications* (Vol. *26*). Sage Publishing.

DeVon, H. A., Block, M. E., Moyle-Wright, P., Ernst, D. M., Hayden, S. J., Lazzara, D. J., Savoy, S. M., & Kostas-Polston, E. (2007). A psychometric toolbox for testing validity and reliability. *Journal of Nursing Scholarship*, *39*(2), 155–164. https://doi.org/10.1111/j.1547-5069.2007.00161.x

Everitt, B. S. (1975). Multivariate analysis: The need for data, and other problems. *British Journal of Psychiatry*, *126*(3), 237–240. https://doi.org/10.1192/bjp.126.3.237

Fabrigar, L. R., & Wegener, D. T. (2011). *Exploratory factor analysis*. Oxford University Press.

Hartigan, L., Cussen, L., Meaney, S., & O'Donoghue, K. (2018). Patients' perception of privacy and confidentiality in the emergency department of a busy obstetric unit. *BMC Health Services Research*, *18*(1), 1–6. https://doi.org/10.1186/s12913-018-3782-6

HIPAA Journal. (2021). *Healthcare data breach statistics*. https://www.hipaajournal.com/healthcare-data-breach-statistics/

SANS Institute. (2021). *Information security resources*. https://www.sans.org/information-security/

Jung, E.-Y., & Jung, S.-J. (2014). A study on perception and practice of protecting the patient medical information in some general hospital employees. *The Korean Journal of Health Service Management*, *8*(4), 35–45. https://doi.org/10.12811/KSHSM.2014.8.4.035

Kaiser, H. F. (1958). The varimax criterion for analytic rotation in factor analysis. *Psychometrika*, *23*(3), 187–200. https://doi.org/10.1007/BF02289233

Kang, J., & Seomun, G. (2021). Information security in nursing: A concept analysis. *Advances in Nursing Science*, *44*(1), 16–30. https://doi.org/10.1097/ANS.0000000000000330

Kim, C.-H., Jeong, S.-Y., & Song, Y. (2013). Recognition and performance of patient private information protection (PPIP) in nursing students. *Journal of Digital Convergence*, *11*(11), 479–490. https://doi.org/10.14400/JDPM.2013.11.11.479

Kim, J. S., & Shin, H. S. (2016). Development of the developmental support competency scale for nurses caring for preterm infants. *Journal of Korean Academy of Nursing*, *46*(6), 793–803. https://doi.org/10.4040/jkan.2016.46.6.793

Kim, M. O. (2012). A study on protecting patients' privacy of obstetric and gynecologic nurses. *Korean Journal of Women Health Nursing*, *18*(4), 268–278. https://doi.org/10.4069/kjwhn.2012.18.4.268

Kim, M. S., & Hunter, J. E. (1993a). Attitude-behavior relations: A meta-analysis of attitudinal relevance and topic. *Journal of Communication*, *43*(1), 101–142. https://doi.org/10.1111/j.1460-2466.1993.tb01251.x

Kim, M. S., & Hunter, J. E. (1993b). Relationships among attitudes, behavioral intentions, and behavior: A meta-analysis of past research, part 2. *Communication Research*, *20*(3), 331–364. https://doi.org/10.1177/009365093020003001

Kinnunen, U.-M., Kuusisto, A., Ahonen, O., Koponen, S., Kaihlanen, A., Hassinen, T., & Vehko, T. (2022). Nurses' informatics competency assessment of health information system usage: A cross-sectional survey. *Research Square*. https://doi.org/10.21203/rs.3.rs-1324459/v1 Preprint (Version 1) available.

Kruse, C. S., Smith, B., Vanderlinden, H., & Nealand, A. (2017). Security techniques for the electronic health records. *Journal of Medical Systems*, *41*(8), 127. https://doi.org/10.1007/s10916-017-0778-4

Lee, E. O., Im, N. Y., Park, H. A., Lee, I. S., Kim, J. I., Bae, J. Y., & Lee, S. M. (2009). *Nursing research and statistical analysis*. Soomoonsa Publisher.

Lee, M. Y., & Park, Y. I. (2005). A study on the nurse's perception and performance of protecting patient privacy. *Journal of Korean Clinical Nursing Research*, *11*(1), 7–20.

Lynn, M. R. (1986). Determination and quantification of content validity. *Nursing Research*, *35*(6), 382–386. https://doi.org/10.1097/00006199-198611000-00017

MacMillan, J. (2021). *Infosec strategies and best practices: Gain proficiency in information security using expert-level strategies and best practices*. Packt Publishing.

Mannix, J., Wilkes, L., & Daly, J. (2015). 'Good ethics and moral standing': A qualitative study of aesthetic leadership in clinical nursing practice. *Journal of Clinical Nursing*, *24*(11–12), 1603–1610. https://doi.org/10.1111/jocn.12761

O'Brien, J. A., & Marakas, G. M. (2006). *Management information systems* (Vol. *6*). McGraw-Hill/Irwin.

Oh, A. S. (2015). A study on home healthcare convergence for IEEE 11073 standard. *Journal of the Korea Institute of Information and Communication Engineering*, *19*(2), 422–427. https://doi.org/10.6109/jkiice.2015.19.2.422

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 & Security*, *66*, 40–51. https://doi.org/10.1016/j.cose.2017.01.004

Rouleau, G., Gagnon, M. P., Côté, J., Payne-Gagnon, J., Hudson, E., & Dubois, C. A. (2017). Impact of information and communication technologies on nursing care: Results of an overview of systematic reviews. *Journal of Medical Internet Research*, *19*(4), e122. https://doi.org/10.2196/jmir.6686

Smaradottir, B. F. (2017, December 14–17). *Security management in health care information systems-A literature review*. Paper presented at the International Conference on Computational Science and Computational Intelligence, Las Vegas, Nevada. https://doi.org/10.1109/CSCI.2017.303

van der Wens, C. (2019). *ISO 27001 handbook: Implementing and auditing an information security management system in small and medium-sized businesses*. Deseo.

Velki, T., Solic, K., & Ocevcic, H. (2014). *Development of users' information security awareness questionnaire (UISAQ)—Ongoing work*. Paper presented at the 37th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), Opatija, Croatia. https://doi.org/10.1109/MIPRO.2014.6859789

Virtanen, L., Kaihlanen, A.-M., Laukka, E., Gluschkoff, K., & Heponiemi, T. (2021). Behavior change techniques to promote healthcare professionals' eHealth competency: A systematic review of interventions. *International Journal of Medical Informatics*, *149*, 104432. https://doi.org/10.1016/j.ijmedinf.2021.104432

Woo, J. P. (2016). *Structural equation model concept and understanding*. Hanarea Academy.

How to cite this article: Kang, J., & Seomun, G. (2023). Development and validation of the information security attitude questionnaire (ISA-Q) for nurses. *Nursing Open*, *10*, 850–860. https://doi.org/10.1002/nop2.1353