Accepted Manuscript online: 2024-09-30 Article published online: 2025-01-15



# Development and Validation of the Nursing Information Security Questionnaire

Xiaoyun Zhou[1] Xiujuan Jing[2] Tingting Gao[2] Hong Liu[2] Xuebing Jing[2]

[1] Department of Nursing Faculty, Shandong Second Medical University, Weifang, Shandong, China
[2] Zibo Central Hospital, Zibo, Shandong, China

Address for correspondence Xuebing Jing, MRes, Zibo Central Hospital, No. 10 Shanghai Road, Zhangdian District, Zibo City, Shandong Province, China (e-mail: jingxuebing@163.com).

Appl Clin Inform 2025;16:44–55.

## Abstract

**Background** Ensuring the security of nursing information holds substantial importance to nursing outcomes and healthcare system management. The awareness of information security among nurses in China is generally inadequate, and there is a lack of standardized evaluation tools for nurse information security in nursing practice. The nursing sector necessitates the establishment of a robust culture surrounding information security.

**Objective** The aim of this study was to construct a self-reporting instrument for evaluating nursing information security.

**Methods** The research team utilized literature analysis and group discussions to draft the item pool. After two rounds of Delphi consultation by 15 experts and pilot testing, the initial questionnaire was formed. Item analysis was carried out on the questionnaire, and the validity and reliability of the instrument were statistically tested by computing the Keiser–Meier–Olkin and Bartlett's tests, an exploratory factor analysis (EFA), a confirmatory factor analysis (CFA), convergent and discriminative validity, descriptive statistics, Cronbach's $\alpha$, and test–retest reliability.

**Results** A total of 501 nurses participated in the study, supplemented by the inclusion of five experts who were invited to contribute to the assessment of content validity. Four factors were formed using EFA ($n = 250$), and the cumulative variance contribution rate was found to be 60.10%. The CFA ($n = 251$) showed that the model fit was good. The overall Cronbach's $\alpha$ coefficient of the questionnaire was 0.948, and the test–retest reliability was 0.837.

**Conclusion** Finally, the nursing information security questionnaire (NIS-Q) with 38 items and three dimensions of knowledge, attitude, and practice were formed. A promising assessment instrument for gauging the degree of nursing information security was introduced. Further, a foundational platform was established for implementing specific enhancement strategies aimed at advancing nursing information security.

**Keywords**

- nursing
- information security
- knowledge
- attitude and practice
- validation
- reliability

**received**
July 10, 2024
**accepted after revision**
September 24, 2024
**accepted manuscript online**
September 30, 2024

DOI https://doi.org/10.1055/a-2424-2103.
ISSN 1869-0327.



Georg Thieme Verlag KG, Rüdigerstraße 14, 70469 Stuttgart, Germany

## Background and Significance

Information security comprises three elements: confidentiality, integrity, and availability.[1] The lack of adequate regulations in Chinese medical institutions regarding the protection of clinical health data poses challenges to nursing information security. One case occurred in 2020, where two obstetrical nurses in a Chinese hospital illegally leaked thousands of maternal staff information, resulting in frequent harassment of maternal staff via text messages and phone calls.[2] In addition, with the huge scale of health big data of "Internet + nursing service," the privacy and medical information contained in the data about nurses and patients may be illegally obtained if a cyberattack occurs.[3] These breaches inflict the confidentiality, and availability of information is compromised. According to surveys, 96.64% of nurses believe that emergency drills are very helpful for dealing with network and information security emergencies or major software and hardware failures. Such drills can improve the emergency response speed and decision-making ability of clinical nurses for nursing information, to maintain the integrity of data.[4]

Threats to the safety of health care data need much more focused attention than they have received in the past.[5] As such, ensuring the security of health information has emerged as a significant challenge.[6–8] The awareness of information security among nurses in China is generally inadequate. Due to the shortage of nurses and inadequate nursing information systems, Chinese nurses often resort to using unauthorized social software such as WeChat, DingDing, and email for disseminating patient information and shift updates. However, they may not be aware of the potential impact on information security. And there is a lack of standardized evaluation tools for nurse information security in nursing practice. The nursing sector necessitates the establishment of a robust culture surrounding information security. Dr. David Blumenthal highlighted that the security of health care information requires joint efforts of medical institutions and health care staff.[5,9] Similarly, for care information security, in addition to actions at the level of a health care institution or organization regarding the hospital information system, as the primary provider of care service, nurses' adherence to information security protocols assumes a pivotal role in upholding overall information security.[10,11] Therefore, maintaining the security of nursing information also requires the efforts of the nurse community. The security of nursing information is pivotal in preventing incidents such as data deletion, tampering, and unauthorized access within information systems, which directly affect the quality and effectiveness of nursing work.[12] However, there is no uniform definition of nursing information security. Kang and Seomun[13] conducted a conceptual analysis of nursing information security in 2021, and defined nursing information security as "attitudes of nurses to deepen their awareness of the importance of medical information and to prevent information disclosure by considering technical, physical, and administrative aspects." It only emphasizes the prevention of information leakage but this is not comprehensive. The utilization of specific instruments can be employed to assess the extent of information security among nurses. Kang and Seomun[10] compiled a nurses' information security attitude questionnaire. This particular questionnaire can be utilized for the purpose of investigating the attitudes held by nurses. This questionnaire was not developed by following a thorough definition. Magdalinou et al[14] surveyed 165 nurses in Greek hospitals using an adapted version of the Human Aspects of Information Security Questionnaire (HAIS-Q).[15] The research did not have a well-developed theoretical framework, and the questionnaire was not specific to nurses. The field of nursing information security in China is still in its early stages, primarily concerning nurses' attitudes towards information security and their level of knowledge, with a lack of dedicated assessment tools for nurses.

The security of nursing information plays a crucial role in mitigating nurse–patient disputes and enhancing nurses' operational efficiency and the quality of care they provide. Currently, however, there is no mature concept and suitable theoretical framework to guide the construction of instruments. Moreover, there is currently an absence of a reliable and effective tool for assessing the level of information security in nursing care. Therefore, this study is purposed to construct and evaluate a self-reporting tool for nursing information security from the perspective of nurses and enhance nursing information security behavior.

## Methods

This study covered four phases : conceptualization, item pool development, development of preliminary questionnaire, and development of the nursing information security questionnaire (NIS-Q). The paper "Essential elements of questionnaire design and development" provides a logical, systematic, and structured approach to questionnaire design and development, and explores the process by which a reliable and valid questionnaire can be developed.[16] We followed these approaches with a view to develop the present instrument.[8] To assure content validity, the research team followed the research guidelines for the Delphi survey technique and carried out two rounds of Delphi expert consultation.[17] ►Fig. 1 shows the flowchart of this study.

### Study Design and Participants

According to the feedback received from the experts in the Delphi phase,[18] the research team formulated a preliminary questionnaire of the Nursing Information Security. Then, the reliability and validity of the preliminary questionnaire were evaluated based on a cross-sectional survey.

The sample size had to be at least five times the number of items, which, in this case, amounted to 200.[19] Since the preliminary questionnaire consisted of 40 items, and considering an estimated 10% attrition rate, the aim was to recruit a minimum of 220 participants. Moreover, an additional minimum of 200 cases was necessary for conducting confirmatory factor analysis (CFA). Therefore, the participants were randomly divided into two halves, with Sample 1

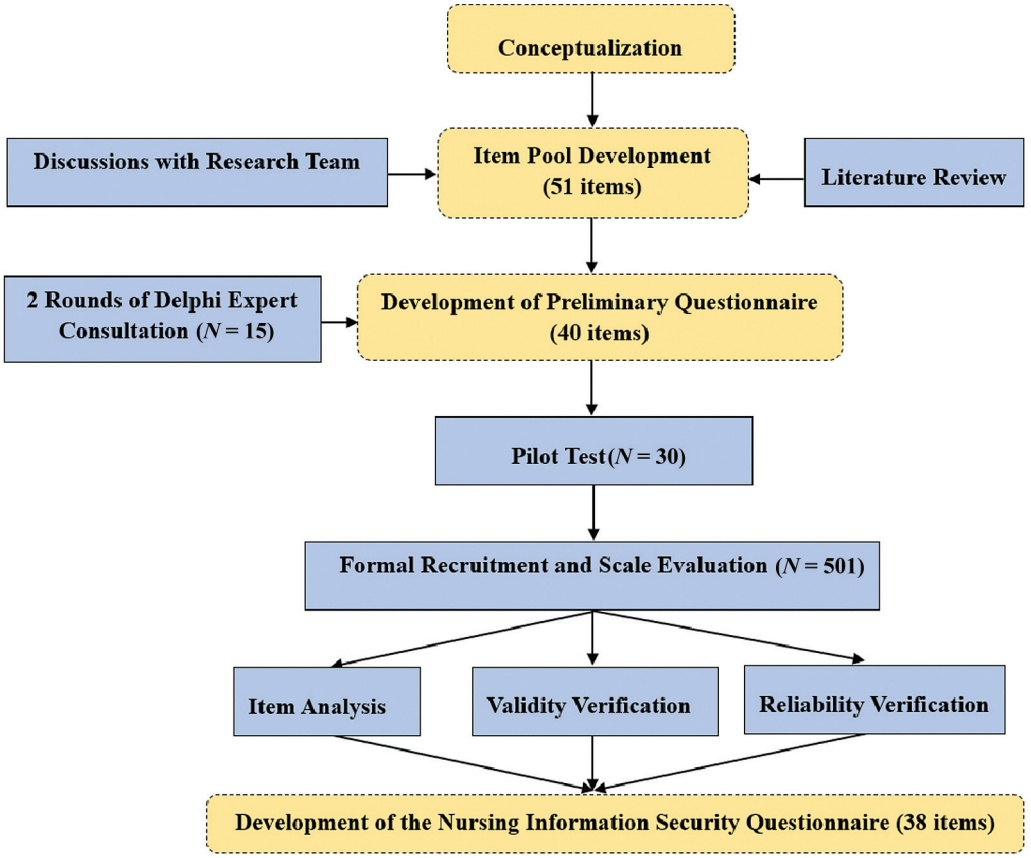


**Fig. 1** Flowchart of this study.

being used for item analysis, exploratory factor analysis (EFA), and analysis of internal consistency, and Sample 2 being used for CFA, convergent and discriminative validity. Participants recruited via convenience sampling had to meet the following inclusion criteria: (1) nurses with a professional qualification certificate in nursing; (2) over 12 months of experience in a tertiary general hospital; and (3) informed consent and voluntary participation. In addition, off-duty nurses were excluded.

## Data Collection

The formal recruitment began in June 2023 and included online and offline recruitment. The research team provided access to the electronic questionnaire as well as a paper version for participants to complete. In addition to the investigator's hospital, the participants were sampled from five tertiary general hospitals in China, and hospitals were selected based on convenience sampling. The directors of nursing departments or head nurses from these five hospitals were contacted beforehand via WeChat or email. This communication aimed to elucidate the study's objectives and intentions. The directors would send the link to the questionnaire in the relevant work groups, and interested nurses would volunteer for the test. To ensure accuracy, each internet protocol (IP) address was limited to submitting responses only once. As for the offline questionnaires, the research team visited various departments of their own hospital to distribute paper questionnaires and explain the study objective, and nurses participated voluntarily. Both the online and offline questionnaires included 9 general information questions and 40 items of preliminary NIS-Q.

## Conceptualization

The initial step of developing a new questionnaire is to define the concept to be measured.[20] Nursing information refers to all the information related to nursing,[21] for example, patients' health information, patients' privacy, nursing records, and other work information. Privacy is patients' right to have full control of their data.[22] Confidentiality and integrity of patient information are crucial to ensuring that patients' privacy is respected and high-quality care is provided.[21] As for sensitive clinical data, professionals who have access to patient records have an ethical/legal obligation to hold that information in confidence.[22,23] The three pillars that uphold the security of protected health information as outlined by the Health Insurance Portability and Accountability Act (HIPAA) are access, administrative, and physical safeguards.[24] On this basis, Kang and Seomun[13] conducted a concept analysis, the definition of information security in nursing was derived as follows: "Attitudes of nurses to deepen their awareness of the importance of medical information and to prevent information disclosure by considering technical, physical, and administrative aspects." A total of seven attributes of information security in nursing were derived. The physical security aspect included two types: "facility stability" and "environmental

control." Technical security has two types: "information accessibility" and "taking advantage of features." The administrative security aspect consisted of three types: "systematicity of work," "execution of education," and "professional responsibility." Ge et al[25] took the ability to protect privacy and information security as one of the training goals in the master of nursing specialist in the field of health informatics. The specific requirements were to train students to understand and comply with relevant laws, regulations, and ethical guidelines, and to protect patients' privacy and information security. Because this study is purposed to develop a self-reporting tool for nurses; based on the above, the nursing information security in this study is defined as nurses understanding relevant laws and regulations, abiding by professional ethics, keeping work information confidential, protecting patients' privacy, and preventing information disclosure by considering access, technical, physical, and administrative aspects.

### Item Pool Development

The item pool is constructed mainly through a literature review and the research team's discussion. The research team discussed and identified search terms, such as "nurse," "nursing," "information security," "informatization," and "information system," and the relevant literature was reviewed and analyzed.[13,14,26–29] As found in the literature review, a positive correlation exists between nurses' practice behavior in information security and their knowledge and attitude towards information security.[14] Therefore, we want to comprehensively evaluate nurses' knowledge, attitude, and practice. In the setting of the questionnaire's dimensions, it was framed by the knowledge–attitude–practice theory, including three dimensions: knowledge, attitude, and practice. For specific items in each dimension, based on a conceptual analysis of nursing information security, we created the items. In other words, the content of each item maps certain connotations of the conceptual analysis. Furthermore, we referred to the information security attitude questionnaire (ISA-Q), as well as other instruments that are used to investigate nursing information security attitudes.[10,14] This approach produced an initial pool of 51 items (17 items in each dimension) rated using a 5-point Likert scale ranging from 1 (strongly disagree) to 5 (strongly agree).

### Expert Consultation

Expert consultation questionnaires were prepared based on the item pool. The Delphi method was used for two rounds of expert letter consultation. The expert selection criteria were as follows: (1) experts in the fields of nursing management, nursing or nursing informatics; (2) associate senior title or above; (3) over 10 years of professional experience; (4) bachelor's degree or above; and (5) voluntary participation. The scale items were assigned using a 5-point Likert scale, with a score from 1 to 5 indicating "very unimportant" to "very important." The items were selected according to the criteria of importance mean $\geq$0.4 and coefficient of variation $<$0.25.[30] The experts were also asked to point out and comment on poor wording or redundancies in the proposed questions and suggest missing questions. Subsequently, the items were revised according to the collected experts' suggestions and scores.

A preliminary questionnaire was determined, and each item could be scored by means of the 5-point Likert method. A higher score indicated a higher level of nursing information security knowledge attitude and practice.

### Pilot Test

Before the formal recruitment, a preliminary survey was conducted using convenience sampling, involving 30 registered nurses employed at a tertiary general hospital for a minimum of 12 months. The aim of the presurvey was to gather their responses and feedback before the formal assessment. This confirmed the accuracy, readability, and ambiguity of the preliminary questionnaire.[8]

### Item Analysis

Items were screened using the classical test theory,[31] specifically employing the critical ratio method, correlation coefficient method, and Cronbach's $\alpha$ coefficient method. The cumulative scores from the scale were sorted in descending order. The association between the high-scoring group (top 27%) and the low-scoring group (bottom 27%) was examined. Subsequently, each individual item's mean was compared to determine the extent of discrimination within the questionnaire. If the correlation coefficient between items and total scores was less than 0.4, the item needed to be deleted.[32] In the event that removing an item resulted in an increase in the overall Cronbach's $\alpha$ coefficient, it indicated that said item had an Impact on the internal consistency of the questionnaire. Consequently, the item would be deleted.[33]

### Validity Verification

The validity tests of the NIS-Q content validity, concerned structure validity, convergent validity, and discriminative validity.

In the present study, EFA and CFA were used to evaluate the structural validity of the questionnaire. Before conducting EFA, Bartlett's sphericity test was executed, and the Kaiser–Meyer–Olkin (KMO) index was assessed. EFA was then conducted utilizing the principal component analysis method with varimax rotation. The aim was to unveil the underlying structure of the questionnaire.[30]

The average variance extraction (AVE) and combined reliability (CR) of each factor were calculated to evaluate the convergent and discriminative validity. An AVE value exceeding 0.5 and a CR value surpassing 0.7 would indicate satisfactory inherent validity.[34]

Five experts were invited to participate in the content validity assessment, including two experts in nursing informatics and three experts in nursing. A 4-point Likert scale was used to score the relevance of each item, where 1 to 4 indicated "no correlation" to "perfect correlation," to calculate the item-level content validity index (I-CVI) and the scale-level content validity index (S-CVI). Each I-CVI was calculated based on the number of experts scoring either 3 or

4, and the S-CVI was defined as "the proportion of items on an instrument that achieved a rating of 3 or 4 by all the content experts."[33] I-CVI at or above 0.78 and S-CVI at or above 0.80 are generally considered acceptable.[35]

### Reliability Verification

The reliability verification of the present study included internal consistency and test–retest reliability, and all results were expressed using Cronbach's coefficient. Two weeks after the formal test, 20 of the nurses who had participated in the test were selected to refill the questionnaire to calculate the test–retest reliability. In order to ensure the representativeness of the sample, we adopted a random sampling method.

### Ethical Considerations

This study was approved by the ethical review of the Zibo Central Hospital Ethics Committee (approval no.: 2023049). Informed consent was obtained from the participating nurses. Those recruited online were unable to proceed until they had read the informed consent form and clicked the "informed consent" button. For offline recruits, signing a physical informed consent form was mandatory. Nurses were told that participation was voluntary and that they could withdraw at any time. The nurses' information was kept anonymous and completely confidential, and all data were used for the present study only.

## Results

Fifteen experts participated in two rounds of Delphi expert consultations. The specialists were aged 37 to 57 ($45.60 \pm 5.34$) years and had 10 to 39 ($22.80 \pm 9.75$) years of work experience. Among the 15 experts, there were 10 nursing management experts (five of them are nurse managers on the hospital's information management committee), 2 nursing education experts, 2 clinical nursing experts, and 1 nursing information expert. Their educational level was bachelor's degree ($n = 4$), master's degree ($n = 10$), and doctor ($n = 1$). After adding, modifying, merging, and deleting items according to two rounds of expert opinions, 40 items remained. The primary questionnaire was developed based on these 40 items, which contained 13 items about knowledge (K1–K13), 11 items about attitude (A1–A11), and 16 items about practice (P1–P16).

A pilot test was administered to 20 nurses at the investigator's hospital. There were 2 (10%) males and 18 (90%) females, and the age of the nurses ranged from 26 to 44 years. Two participants (10%) were engaged in nursing management and the other 18 (90%) participants were nurses. Based on their feedback after answering the questionnaire, the details that were difficult to understand were revised and brief explanations were added.

A total of 549 nurses participated in the formal survey, and the data were carefully reviewed and entered by two investigators, leading to the removal of invalid questionnaires. Ultimately, 501 valid questionnaires were recovered, with an effective recovery rate of 91.26%. Of the 501 valid study participants, 452 (90.2%) were female, and most of them ($n = 204$, 40.7%) were senior nurses. About half ($n = 255$, 50.9%) of the nurses had experienced training involving information security. The average age of the respondents was $29.54 \pm 5.88$ years, and the vast majority ($n = 398$, 79.44%) had undergraduate degrees (►Table 1).

The results of the critical ratio method, correlation coefficient method, and Cronbach's $\alpha$ coefficient method are as follows: The critical ratio method showed that the results of the independent-sample $t$-test for all the items in the high and low groups were between 6.30 and 22.90, which was statistically significant ($p < 0.05$). The correlation coefficient of each item and the total score was distributed between 0.41 and 0.78, which was confirmed to be above 0.30. The Cronbach's coefficient did not increase significantly after deleting any one item separately. Thus, the 40 items had good homogeneity and discrimination and were retained to test construct validity.

The content validity of the questionnaire was good. For I-CVI, it ranged from 0.80 to 1. For S-CVI, it was 0.94. Both of them met the criteria.

The KMO value of sample 1 was high (0.94), and Bartlett's test of sphericity showed a significant $p$-value ($\chi^2 = 6{,}768.39$, $p < 0.0001$). Both indicate that the data were appropriate for EFA. EFA was mainly used to reevaluate and filter items, and it was conducted on the preliminary questionnaire of 40 items. A procedure was followed to ensure that the factors were stable across the extraction and rotation methods. The result of EFA shows that two items (P2 and P4) were excluded due to having factors comprising less than three items. In other words, these two items have created a dimension on their own. All loadings of the remaining items were above the traditional cutoff value of 0.40. Factor 1 was named Practice because it included amounting to a total of 14 items about practice P1, P3, and P5–P16. Similarly, Factor 2 was named Attitude because it included 11 items about attitudes. Factor 3 contained the knowledge-related items K1 to K7, and Factor 4 contained the knowledge-related items K8 to K13. Both factors were related to knowledge and were thus named Knowledge a and Knowledge b, respectively. The results show that the variance contribution rates of the four factors were 13.25, 4.23, 3.68, and 1.68%, respectively, and the cumulative variance contribution rate was 60.10%. ►Table 2 provides further details.

Based on the EFA screening items, CFA evaluates the entire model and filters the problematic items again. The goodness of fit of the model structure was validated using 251 samples from Sample 2 (►Fig. 2). The maximum likelihood estimation method suggested that the fitting indexes of the four-factor model reached the reference value and the model fit well, and the CMIN/DF (Discrepancy Divided by Degree of Freedom) = 1.254 < 3, AGFI (Adjusted Goodness of Fit Index) = 0.841 > 0.8, RMSEA (Root Mean Square Error of Approximation) = 0.032 < 0.08, CFI (Compare Fit Index) = 0.975 > 0.90, GFI (Goodness of Fit Index) = 0.975 > 0.90, TLI (Tucker Lewis Index) = 0.974 > 0.90.

The CR of the questionnaire was 0.91 to 0.95, which met the criterion of 0.7 or higher. The AVE ranged from 0.59 to 0.61. The correlation coefficient between factors revealed by the discriminant validity test is shown in ►Table 3. After

**Table 1** Characteristics of participants ($n = 501$)

| Variables | Mean ± SD (range) or *n* (%) | |
|---|---|---|
| Sex | Female | 49 (9.8%) |
| | Male | 452 (90.2%) |
| Age, y | 29.54 ± 5.88 | |
| | 20–29 | 301 (60.1%) |
| | 30–39 | 163 (32.5%) |
| | ≥40 | 37 (7.4%) |
| Years of nursing experience | 1–5 | 273 (54.5%) |
| | 6–10 | 116 (23.2%) |
| | 11–20 | 93 (18.6%) |
| | ≥21 | 19 (3.8%) |
| Positional title | Staff nurse | 138 (27.5%) |
| | Senior nurse | 204 (40.7%) |
| | Supervisor nurse | 150 (29.9%) |
| | Associate chief nurse or above | 9 (1.8%) |
| Position | Nothing | 457 (91.2%) |
| | Assistant to the charge nurse | 25 (5.0%) |
| | charge nurse or above | 19 (3.8%) |
| Level of education | Associate degree | 79 (15.8%) |
| | Bachelor's degree | 398 (79.4%) |
| | Master's degree or above | 24 (4.8%) |
| Experience of clinical teachers | Yes | 203 (40.5%) |
| | No | 298 (59.5%) |
| Experience in nursing information security training was included | Yes | 255 (50.9%) |
| | No | 246 (49.1%) |

Abbreviation: SD, standard deviation.

calculation, the correlation coefficients of any two factors were less than the AVE values of both of these two factors, indicating the discriminant validity was good.

The Cronbach's α reliability coefficients for each dimension of the questionnaire were found to be acceptable. The coefficients obtained for the dimensions of knowledge, attitude, and practice were 0.899, 0.924, and 0.953, respectively. The overall Cronbach's α coefficient was 0.948, which demonstrated that the questionnaire had good internal consistency reliability. Two weeks later, the overall reliability of the retest with 20 nurses was 0.837, and the test–retest reliability of each dimension ranged from 0.880 to 0.929. After analysis, the reliability of the questionnaire was good.

The results of the analyses revealed that the validity and reliability levels of the final version of the questionnaire with 38 items were high.

## Discussion

There is still a lack of systematic special training and education on information security in China. In many cases, nurses begin to learn information security only after they do their jobs. In contrast, foreign countries list information security as a special course during the school or training period, so as to improve the safety awareness of medical staff in advance.[36] Information security is affected by environmental factors, information equipment, information technology, and personnel cognition, among others. Personnel may undermine information security due to insufficient knowledge on information security. For example, health care workers may use unauthorized tools to communicate information because hospital equipment is inadequate. They may use WeChat, SMS, and other tools to communicate and disseminate patients' medical messages, thus inadvertently and unknowingly leading to the leakage of patients' information. They may even hold the following misunderstanding: what they are adopting is a more convenient way.[29] Moreover, the awareness of information security in nursing practice among nurses is generally insufficient, and the organization lacks standardized behavior regarding nursing information security. The present study is the first in which an instrument was constructed for assessing the level of nursing information security in China. Partial items in the questionnaire were prepared in a specific Chinese context, so they have Chinese characteristics. For example, K1 involves China's laws and regulations; in P11, the setting of relevant departments of

**Table 2** Exploratory factor analysis ($n = 250$)

| Factor | Items | Factor loading | | | |
|---|---|---|---|---|---|
| | | 1 | 2 | 3 | 4 |
| Practice | P3. I will promptly switch to my own account upon logging into the nursing work system. | 0.799 | 0.188 | 0.128 | 0.059 |
| | P14. I will not copy, transmit or share the hospital's medical or nursing information without permission. | 0.773 | 0.143 | 0.136 | 0.191 |
| | P6. I will prevent other unauthorized persons from accessing medical and nursing records. | 0.773 | 0.166 | 0.032 | 0.015 |
| | P5. I will not utilize the hospital's network resources or access information without authorization. If necessary for work or research, I will apply for patient information in accordance with regulations. | 0.766 | 0.179 | 0.017 | 0.075 |
| | P10. I will help rotating nurses, continuing education nurses and nursing students avoid actions that pose information security risks. | 0.766 | 0.152 | 0.169 | 0.052 |
| | P15. I will not dismantle, install or debug software or hardware on any office computer by myself. | 0.763 | 0.202 | 0.159 | 0.187 |
| | P16. I will actively participate in various emergency response drills organized by managers, so as to deal with equipment failures and network collapses. | 0.752 | 0.197 | 0.163 | 0.052 |
| | P9. I will not disclose the hospital's information (such as the specific name, specifications, and models of drugs or consumables) to manufacturers or medical representatives. | 0.752 | 0.092 | 0.062 | 0.101 |
| | P8. When conducting activities such as nursing rounds, medical record reporting, I will mosaic or conceal any private information that is not relevant to the patient's condition. | 0.749 | 0.189 | 0.169 | 0.090 |
| | P13. I will not disclose patient information to anyone not involved in medical activities without the patient's consent. | 0.746 | 0.216 | 0.116 | 0.082 |
| | P12. I actively participate in information security training activities organized by managers. | 0.741 | 0.203 | 0.188 | 0.049 |
| | P7. I will prevent patients, family members, and other non-staff members from accessing the hospital network. | 0.739 | 0.209 | −0.006 | 0.193 |
| | P11. Upon discovering issues with information equipment, I will promptly consult with professionals (Information Department, Equipment Department, Logistics Supply Department) to prevent any potential information leakage. | 0.724 | 0.229 | 0.135 | 0.022 |
| | P1. I will abide by the relevant laws and regulations of information security and the relevant rules and regulations of the hospital in my work. | 0.689 | 0.259 | 0.006 | 0.210 |
| Attitude | A9. I think it's very important to conduct various emergency response drills to deal with equipment failures and network paralysis. | 0.191 | 0.765 | 0.020 | 0.248 |
| | A11. I think it is not advisable to access patient information when not engaged in work or study. | 0.151 | 0.765 | 0.096 | 0.145 |
| | A8. I think it's important to conduct a clinical information security risk assessment. | 0.187 | 0.757 | 0.111 | 0.102 |
| | A10. I think technology support is important in promoting nursing information security. | 0.149 | 0.753 | 0.024 | 0.225 |
| | A1. I think that nursing information security is extremely important and constitutes a critical component of hospital information security | 0.077 | 0.742 | −0.060 | 0.174 |
| | A2. I believe that protecting the nursing information security is conducive to the orderly development of nursing work and safeguarding the legitimate rights and interests of nursing staff. | 0.219 | 0.724 | 0.077 | 0.033 |

**Table 2** (*Continued*)

| Factor | Items | Factor loading | | | |
|---|---|---|---|---|---|
| | | 1 | 2 | 3 | 4 |
| | A7. I think it's important to take preventive measures to prevent information loss and leakage in clinical nursing work. | 0.189 | 0.685 | 0.161 | 0.067 |
| | A6. I believe it's very necessary to abide by the laws and regulations of information security and the hospital's information security management system in the work process. | 0.232 | 0.685 | 0.199 | 0.021 |
| | A3. I believe that clinical nursing information security can influence patient outcomes. | 0.233 | 0.663 | −0.022 | 0.103 |
| | A4. I am willing to proactively learn about nursing information security. | 0.285 | 0.659 | 0.088 | −0.009 |
| | A5. I am willing to proactively undergo training on nursing information security. | 0.271 | 0.629 | 0.043 | 0.155 |
| Knowledge | K3. I am aware that nursing information security has independent theory and content. | 0.140 | 0.095 | 0.819 | 0.060 |
| | K5. I understand that technical security measures protect information data, control access to information system, and utilize software to enhance security. | 0.095 | 0.025 | 0.766 | 0.154 |
| | K1. I understand that China has laws and regulations pertinent to information security (Data Security Law of the People's Republic of China, Personal Information Protection Law of the People's Republic of China, etc.). | 0.212 | 0.079 | 0.745 | 0.126 |
| | K6. I understand that the management security level represents a macro security measure, encompassing laws, education, systems, and security plans. | 0.066 | 0.032 | 0.696 | 0.315 |
| | K4. I understand that physical security measures should be taken to ensure the integrity of information equipment and protect information systems against unauthorized access and malicious damage. | 0.114 | 0.146 | 0.675 | 0.299 |
| | K2. I am aware of the hospital's current information security management system. | 0.202 | 0.077 | 0.655 | 0.156 |
| | K7. I understand that to protect data security, virus prevention and software maintenance should be done regularly in software management. | 0.055 | 0.062 | 0.636 | 0.328 |
| | K10. I understand that important data should be backed up and properly managed to prevent loss. | 0.058 | 0.237 | 0.208 | 0.718 |
| | K12. I understand that nursing information security capabilities can be improved through education and training. | 0.206 | 0.211 | 0.274 | 0.696 |
| | K13. I understand that nursing information security is a responsibility that nurses must master and implement during their professional practice. | 0.128 | 0.200 | 0.183 | 0.692 |
| | K11. I understand that nursing information security requires strict management of access rights to information to prevent misuse of data. | 0.166 | 0.126 | 0.126 | 0.689 |
| | K8. I understand that management personnel may assign specialized staff for inspection and maintenance of hardware facilities and equipment, ensuring they are in good condition. | 0.089 | 0.061 | 0.322 | 0.689 |
| | K9. I understand the emergency response strategies for emergencies that result in equipment failure or network paralysis. | 0.135 | 0.126 | 0.270 | 0.632 |

hospitals might vary from country to country. When using this scale in different cultural contexts, adjustments are needed. At present, there is a lack of a mature definition of nursing information security. Therefore, this study conceptualizes the nursing information security from the perspective of nurses. This is an innovation of this study. Moreover, KAP (Knowledge-attitude-practice) theory is introduced in the setting of dimensions, the NIS-Q can evaluate the level of

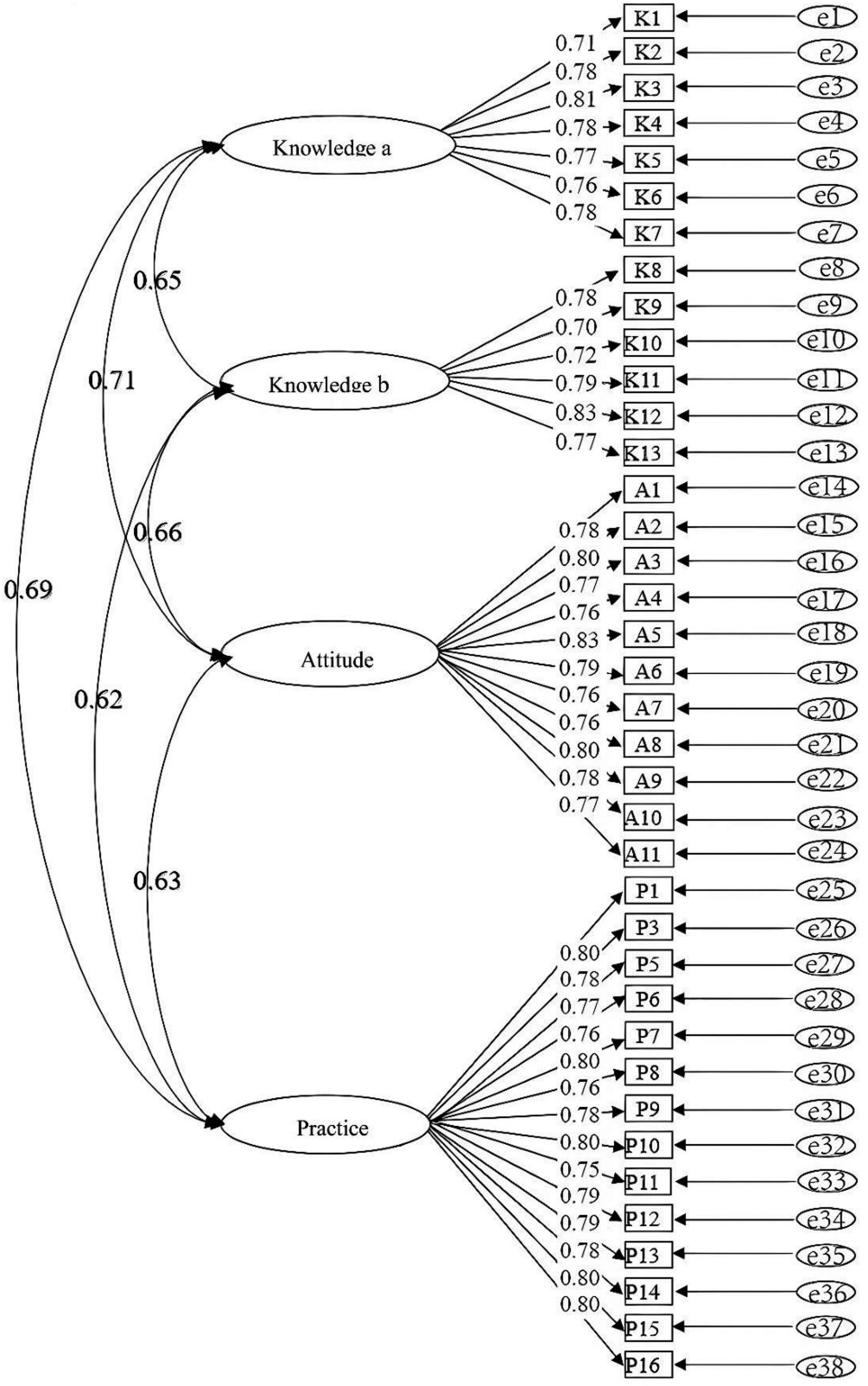


**Fig. 2** Model for confirmatory factor analysis of the KAP-NIS-Q ($n = 251$). NIS-Q, nursing information security questionnaire.

nursing security-related knowledge, attitude, and practice comprehensively. In essence, effective information security practices require nurses to possess a sound understanding and favorable attitude towards nursing information security.[14,37] The NIS-Q provides a basis for conducting targeted educational improvement projects.

Some similar studies used questionnaires to survey nurses' level of nursing information security. Magdalinou

**Table 3** Convergent validity and discriminative validity analysis

| | F1 | F2 | F3 | F4 | AVE |
|---|---|---|---|---|---|
| F1 | 1 | | | | 0.59 |
| F2 | 0.65[a] | 1 | | | 0.59 |
| F3 | 0.71[a] | 0.66[a] | 1 | | 0.61 |
| F4 | 0.69[a] | 0.62[a] | 0.63[a] | 1 | 0.61 |

Abbreviation: AVE, average variance extraction.
[a]$p < 0.05$.

et al[14] developed an instrument that was related to the policies and procedures of information security, which is different from the content of the questionnaire in the present study. Its theoretical foundation lies in the self-reporting perception of danger, training opportunities, the enforcement of IT security policies, and the culture in the organization that can affect employees' IT security practices by examining the nurses' non-secure IT practices. This is different from this study, which is based on the research team's conceptual analysis of nursing information security. In addition, in terms of research methodology, it assesses the internal consistency of the tool only. This study makes complete item analysis, validity verification, and reliability verification. Based on their own research team's conceptual analysis of nursing information security,[13] Kang and Seomun[10] developed the nurses' information security attitude questionnaire. The concept analysis contained seven attributes: within the physical aspect were environmental control and facility stability; the technical aspect comprised information accessibility and leveraging features while the administrative aspect included work systematicity, educational execution, and professional responsibility. Kang and Seomun[10] extracted six dimensions directly from these three dimensions and seven attributes. In addition to the differences in conceptual analysis, this study refers to the KAP theory for the setting of dimensions based on the results of the literature review. The three dimensions of the questionnaire, that is, knowledge, attitude, and practice, can comprehensively investigate nurses' levels of knowledge, attitude, and practice about nursing information security. In contrast, the questionnaire prepared by Kang and Seomun[10] is used only to investigate nurses' attitudes. However, there are some similarities between this study and the other research. In the preparation of each specific item, the study makes reference to the content of the items of the other research, while making a conceptual analysis.

To maintain the scientific rigor of the questionnaire, the initial draft underwent a process involving literature analysis, deliberation within the research team, and two rounds of consultations with 15 nursing experts. The questionnaire was subsequently revised based on the insights provided by these experts. The questionnaire development process was followed and pilot testing and item analysis were conducted. The reliability and validity of the questionnaire were verified. The sample was randomly divided into two groups, ensuring relatively independent sets. These samples were then used for the CFA to ensure the statistical validity of the sample and to meet the required size criteria.[19,38] During the EFA, four factors were examined. Within the knowledge dimension, two factors emerged, referred to as "Knowledge a" and "Knowledge b." The reason may be that the knowledge section of Factor 3 is mainly extracted from institutional regulations and literature, so it is focused more on theoretical knowledge; in contrast, the knowledge section of Factor 4 is mainly related to clinical practice. Different focuses of knowledge content lead to this phenomenon. Following team discussions, the two factors were consolidated into a single dimension termed "Knowledge." The content validity of the questionnaire was above 0.8, which showed good content validity.[39,40] Moreover, the convergent validity and discriminative validity were confirmed to ensure the objectivity of the instrument.[41] After analysis, the reliability of the questionnaire was high. The overall Cronbach's $\alpha$ coefficient reached 0.948 and it was high in all dimensions ($>0.8$).[42]

We encountered challenges during the process of collecting questionnaires. We observed significant variations in the level of nursing IT across hospitals of different grades, as well as disparities between the practices of medical professionals in community and small-scale hospitals compared to general hospitals. In community and small-scale hospitals, insufficient attention is given to nursing information security, with many questionnaire items not being addressed in their daily tasks. For instance, management rules on nursing information security are often lacking, training and education related to information security are inadequate, and essential nursing activities such as rounds and medical record discussions are rarely conducted. Furthermore, their nursing information systems are frequently unusable. Consequently, we found that this questionnaire is more suitable for nurses working in large general hospitals.

## Limitations

There are certain limitations in the present study. Considering that the degree of nursing informatization in small medical institutions is insufficient, the 501 participants were all from tertiary general hospitals, and nurses from other level hospitals were not considered, which may have led to some bias. Additionally, with a convenience sample of just five hospitals across the country, the representation of hospitals may not be typical. In addition, there is a lack of cross-sectional research and influencing factor analysis in large samples about nurses' knowledge, attitude, and

practice related to information security, so no proper bases are available for identifying the defects in nurses' information security management. The results of this study only provide a tool for self-reporting on nursing information security from the perspective of nurses. In the future, in-depth research can be done by health care institutions or organizations regarding the hospital information system.

## Conclusion

In this study, the NIS-Q was developed and its reliability and validity were verified. The NIS-Q demonstrates high levels of reliability and validity, making it a valuable tool for assessing the proficiency level of nursing information security in China. Our model can assist in identifying the knowledge, attitudes, and behaviors related to information security in nursing practice, enhancing the standardization of clinical nurses' information safety behavior, and ensuring a secure medical information environment. Further testing of this newly developed instrument with a larger number of nurses from various backgrounds and different settings is recommended.

## Clinical Relevance Statement

This study used a newly developed instrument with the aim of comprehensive evaluation of clinical nurses' knowledge, attitude, and practice of nursing information security. This study can provide valuable guidance for clinical nurses to improve their information security practice behavior.

## Multiple-Choice Questions

1. Which dimensions are included in the new development tools?
   a. Knowledge
   b. Attitude
   c. Practice
   d. All of the above.

   **Correct Answer:** The correct answer is option d. The questionnaire on information security knowledge, attitude, and practice in nursing provides an instrument for surveying the proficiency level of nursing information security.

2. What was mainly examined of the NIS-Q in this study?
   a. Reliability
   b. Validity
   c. Both a. and b.
   d. Specificity

   **Correct Answer:** The correct answer is option c. The NIS-Q was developed and its reliability and validity were verified.

### Protection of Human and Animal Subjects

This research was approved by the Ethics Committee of Zibo Central Hospital. The participants who volunteered to participate in the study were informed about the subject and purpose of the study and their informed consent was obtained. All participants are anonymous and the privacy of participants has not been exposed.

### Funding

None.

### Conflict of Interest

None declared.

### Acknowledgments

The authors would like to thank all the consulting experts and participants who voluntarily participated in the study.

## References

1 Hou Y. Information security and data sharing in health systems. China High New Technol 2023;(22):139–141
2 Gui Y. Protection study of patient medical information on legal. Yunnan University of Finance and Economics; 2023. Doi: 10.27455/d.cnki.gycmc.2023.000168
3 Liu WJ, Wu CQ, Sun WQ. Study on ethical issues under the Mode of "Internet+ nursing service". Med Philos 2021;42(12):32–35
4 Huang C, Pan HY, Zhuang YY, et al. Construction and effect evaluation of hospital nursing information emergency system. Nurs Rehabil 2023;22(02):53–56
5 Liu V, Musen MA, Chou T. Data breaches of protected health information in the United States. JAMA 2015;313(14):1471–1473
6 Beck EJ, Gill W, De Lay PR. Protecting the confidentiality and security of personal health information in low- and middle-income countries in the era of SDGs and Big Data. Glob Health Action 2016;9:32089
7 Hasselgren A, Hanssen Rensaa JA, Kralevska K, Gligoroski D, Faxvaag A. Blockchain for increased trust in virtual health care: proof-of-concept study. J Med Internet Res 2021;23(07):e28496
8 Sarac E, Yildiz E. Development and validation of information technology scale in nursing. Appl Clin Inform 2024;15(02): 220–229
9 Kessler SR, Pindek S, Kleinman G, Andel SA, Spector PE. Information security climate and the assessment of information security risk among healthcare employees. Health Informatics J 2020;26 (01):461–473
10 Kang J, Seomun G. Development and validation of the information security attitude questionnaire (ISA-Q) for nurses. Nurs Open 2023;10(02):850–860
11 Memarian R, Salsali M, Vanaki Z, Ahmadi F, Hajizadeh E. Professional ethics as an important factor in clinical competency in nursing. Nurs Ethics 2007;14(02):203–214
12 Liang R, Shi GW. Problems and ethical countermeasures of nursing information management. Chin J Modern Med 2014;24 (34):110–112
13 Kang J, Seomun G. Information security in nursing: a concept analysis. ANS Adv Nurs Sci 2021;44(01):16–30
14 Magdalinou A, Kalokairinou A, Malamateniou F, Mantas J. Assessing internal consistency of HAIS-Q: a survey conducted in Greek hospitals. Stud Health Technol Inform 2022;295:24–27
15 Parsons K, McCormac A, Butavicius M, et al. Determining employee awareness using the human aspects of information security questionnaire (HAIS-Q). Comput Secur 2014;42:165–176
16 Rattray J, Jones MC. Essential elements of questionnaire design and development. J Clin Nurs 2007;16(02):234–243
17 Hasson F, Keeney S, McKenna H. Research guidelines for the Delphi survey technique. J Adv Nurs 2000;32(04):1008–1015
18 Farzandipour M, Nabovati E, Heidarzadeh Arani M, Akbari H, Sharif R, Anvari S. Enhancing asthma patients' self-management

through smartphone-based application: design, usability evaluation, and educational intervention. Appl Clin Inform 2019;10(05):870–878
19 Wu ML. Practice of questionnaire statistical analysis: SPSS operation and application. Chongqing University Press; 2010:483–490
20 Wang L, Zhang X, Zhang P, Zhou Q, Wang Q, Cheng J. Development and psychometric evaluation of the trauma nurse core competency scale. Front Public Health 2022;10:959176
21 Strachan H. Nursing information. Res Theory Nurs Pract 2002;16(04):287–289
22 Bani Issa W, Al Akour I, Ibrahim A, et al. Privacy, confidentiality, security and patient safety concerns about electronic health records. Int Nurs Rev 2020;67(02):218–230
23 Ciacci G. [Use of data: legal and ethical aspects]. Recenti Prog Med 2015;106(09):455–470
24 Kruse CS, Smith B, Vanderlinden H, Nealand A. Security techniques for the electronic health records. J Med Syst 2017;41(08):127
25 Ge XY, Jia SM, Hu Y, et al. Exploration and practical research of cultivating postgraduate students with master of nursing specialist in the field of health informatics. Chin J Nurs Educ 2024;21(07):828–834
26 Ködmön J, Csajbók ZE. Információbiztonság az egészségügyben. Orv Hetil 2015;156(27):1075–1080
27 Alhuwail D, Al-Jafar E, Abdulsalam Y, AlDuaij S. Information security awareness and behaviors of health care professionals at public health care facilities. Appl Clin Inform 2021;12(04):924–932
28 Kang P, Kang J, Monsen KA. Nurse information security policy compliance, information competence, and information security attitudes predict information security behavior. Comput Inform Nurs 2023;41(08):595–602
29 Liu MD, Ding SN, Wang JN, et al. Research progress of nursing information security. J Nurs (China) 2024;31(04):33–37
30 Zhu ZX, Li X, Han J, et al. Development and validation of Caregiver Preparedness Scale for PICU Transfer Children. J Nurs Sci 2024;39(15):37–40
31 Cappelleri JC, Jason Lundy J, Hays RD. Overview of classical test theory and item response theory for the quantitative assessment of items in developing patient-reported outcomes measures. Clin Ther 2014;36(05):648–662
32 Wu C, Yan J, Wu J, et al. Development, reliability and validity of infectious disease specialist Nurse's Core competence scale. BMC Nurs 2021;20(01):231
33 Raykov T, Marcoulides GA. On the relationship between classical test theory and item response theory: from one to the other and back. Educ Psychol Meas 2016;76(02):325–338
34 Zhang Q, Li X, Zhang K, et al. Psychometric properties of the Chinese version of the knowledge, attitudes and practices of the incontinence-associated dermatitis questionnaire(C-KAP-IAD-Q) used with Chinese nurses. Int J Nurs Pract 2022;29:e13107
35 Polit DF, Beck CT. The content validity index: are you sure you know what's being reported? Critique and recommendations. Res Nurs Health 2006;29(05):489–497
36 Magdalinou A, Kalokairinou A, Malamateniou F, Mantas J. InfoSec practices-a survey conducted in Greek hospitals. Acta Inform Med 2023;31(01):48–52
37 Lynch D, Jedwab RM, Foster J, et al. Voting with their thumbs: assessing communication technology use by medical, nursing, midwifery, and allied health clinicians. Appl Clin Inform 2022;13(04):916–927
38 Ho NAD, Babel S. Electrochemical reduction of different Ag(i)-containing solutions in bioelectrochemical systems for recovery of silver and simultaneous power generation. RSC Adv 2019;9(52):30259–30268
39 Niakan S, Shamshiri A, Davoodi M, Allahyari S. Knowledge and practice of Iranian prosthodontists regarding the diagnosis and treatment of sleep apnea: Design and development of a questionnaire. Dent Res J (Isfahan) 2023;20:19
40 Almanasreh E, Moles R, Chen TF. Evaluation of methods used for estimating content validity. Res Social Adm Pharm 2019;15(02):214–221
41 Jang SM, Kim J. Development of nursing informatics competence scale for Korean nurses. Comput Inform Nurs 2022;40(10):725–733
42 Wijesinghe V, Amaradivakara P, Farukan R. Validation of the Sinhala translations of the pelvic floor distress inventory and the pelvic floor impact questionnaire in a Sri Lankan population. Int Urogynecol J 2021;32(12):3235–3248