Information Technology and Management
https://doi.org/10.1007/s10799-022-00362-y

The role of collectivism and moderating effect of IT proficiency on intention to disclose protected health information

Eun Hee Park[1] · Jongwoo Kim[2] · Lynn Wiles[3]

Accepted: 20 February 2022
© The Author(s), under exclusive licence to Springer Science+Business Media, LLC, part of Springer Nature 2022

Abstract
This paper aims to identify and understand factors affecting insiders' intention to disclose patients' medical information and to investigate how these factors affect the intention to disclose. Based on the literature review on deterrence theory and health information security awareness (HISA), we identify relevant factors and develop a research model explaining insiders' intention to disclose patients' health information. We collect data (N = 105) through scenario-based experiments. Results show that two personal factors, collectivism, and IT proficiency, play a significant role in the model. While collectivism affects two components (health information security regulation awareness and punishment severity awareness) of HISA which influences intention to disclose, IT proficiency moderates the relationship between HISA and intention to disclose. In addition, HISA negatively affects reporting assessment and intention to disclose. This paper aims to fill a research gap in understanding factors affecting insiders' intentions to disclose protected health information. We identify and investigate factors (e.g., collectivism, HISA, reporting assessment, and IT proficiency) that may affect insiders' disclosing intentions. We find that collectivism affects two components of HISA which influence reporting assessment and disclosing intention. We also discover that IT proficiency moderates the relationship between HISA and intention to disclose. Our findings suggest that we need to carefully consider personal factors such as collectivistic nature and IT proficiency in managing insiders' security breaches.

Keywords Collectivism · Health information security awareness · Intention to disclose protected health information · IT proficiency · HIPAA · Reporting assessment

1 Introduction

Securing protected health information (PHI) is a critical security issue in healthcare [1]. The Health Insurance Portability and Accountability Act (HIPAA) prescribes standards for healthcare organizations and stakeholders to comply with for the protection of individual's medical records and health information in the U.S [2]. Insider abuse on privacy breach is reported as a prevalent cause of data leaks and accounts for more than 40 percent of the reported security incidents [3]. Discouraging security breaches by insiders is crucial for protecting information security in organizations.

Our study focuses on student nurses that represent a weak security link at healthcare organizations. Compared with professional nurses, students are still developing their internal value systems and may not fully understand the importance of patients' privacy and the impact of the privacy violations [4]. Therefore student nurses instead of professional nurses are the subjects of our study. The same

✉ Jongwoo Kim
jonathan.kim@umb.edu

Eun Hee Park
epark@odu.edu

Lynn Wiles
lwiles@odu.edu

[1] Information Technology and Decision Sciences, Old Dominion University, 2144 Constant Hall, Norfolk, VA 23529, USA

[2] Management Science and Information Systems, University of Massachusetts Boston, 100 Morrissey Blvd., Boston, MA 02125, USA

[3] School of Nursing, Old Dominion University, 205 VA Beach Higher ED Center 1881, Virginia Beach, VA 23453, USA

Published online: 16 March 2022

security standard required by HIPAA to nurses is applied to student nurses who have access to confidential information [5, 6]. The Office for Civil Rights specifies 'student nurses' as patient care providers in a part of their practical training processes [7]. While conducting clinical practices at hospitals, nursing students have the potential to violate HIPAA by disclosing PHI to relevant stakeholders such as family members and friends, because of their incomplete awareness of laws/policies and sanctions, or mistakes [8, 9]. Student nurses as well as physician assistant students undertaking clinical experience as a part of their education programs may violate HIPAA accidentally and unknowingly [6, 10]. Several prior studies reported possibility and actual violation of HIPAA by student nurses. First, Thompson and Bell [6] noted that student nurses may pose a potential risk to information security when they take various modern technologies to clinical settings and inappropriately use the technologies thereby violating HIPAA. Second, Cannon and Caldwell [5] reported an actual case in which a student nurse violated HIPAA by disclosing a patient's parents' occupations and the litigation status with the patient's family. The student nurse was dismissed right after the violation at the healthcare facility. Third, Westrick [11] also reported multiple cases in which student nurses were dismissed from their nursing programs due to HIPAA violations with their misuse of social media such as Facebook. Fourth, according to Erdil and Korkmaz [12], 37 out of 153 student nurses reported ignoring patient privacy as one of the ethical problems they face during their clinical training. Nursing students inadequately posted protected health information (e.g., a portrayal of people, names, dates, or descriptions of procedures) at social network services thereby potentially violating the protection of health information. Under HIPAA, such acts of revealing PHI without a patient's consent are considered a violation of a patient's privacy [2]. Student nurses must assess whether PHI such as patient's medical status ought to be reported, but the intent to disclose has not been explored in prior studies.

This research gap motivates our study and leads to our interest in student nurses' deviant security behavior—specifically, an *intention to disclose patient's PHI*. It refers to an intention to involve in the aberrant behavior that can "harm patients' mental health, financial conditions, and reputation by revealing PHI to stakeholders of an interest" [[4], p 66]. Training about health information security awareness (HISA) can play a significant role in protecting PHI [9]. However, the impact of student nurses' HISA on their disclosing behaviors remains under-investigated [4].

A prior study [4] identified that individual characteristics such as personal norms and self-control play a significant role between HISA and disclosing behavior. Park et al. [4] suggested the need to investigate the influences of other personal and cultural factors on disclosing behaviors. Therefore, we chose to examine two personal factors whose impacts have not been studied: student nurses' collectivistic nature and information technology (IT) proficiency. While collectivistic nature corresponds to individuals' cultural aspect, IT proficiency is one of personal capabilities that may affect disclosing behavior. 'The Code of Ethics for Nurses' (hereafter referred to simply as "the Code") prescribes non-negotiable ethical standard in nurses' work settings and specifies the values, obligations, and duties of the profession [13]. The Code highlights the value of collective efforts to improve ethical work environment [14, 15]. Student nurses' collectivistic nature or belief, in which collective interests should be a priority to individual self-interest [16], can negatively influence security behaviors. To accomplish student nurses' responsibilities, they must master required technologies. IT proficiency indicates the level of mastery of technical knowledge and skills, which include general knowledge, required hardware/software skills, and security-related technical knowledge [17]. IT proficiency can impact nursing students' behaviors, but this concept has not been investigated.

To address these gaps, this study presents conflicting situations in which, although revealing PHI without the patient's consent is a violation of the privacy, communication with the family may enhance the patient's care [14]. This study contributes to medical informatics, health information security research, nursing education, and healthcare management practices. Research questions include:

1. How does collectivism influence health information security awareness (HISA) of student nurses?
2. How do HISA, student nurses' reporting assessment, and IT proficiency affect intention to disclose PHI?

2 Theoretical background and research model

To answer the research questions above, we conduct a literature review on privacy and compliance in healthcare, deterrence theory, and HISA. We further explored to identify factors that explain insiders' non-compliance behavior in the healthcare security context. We identify collectivism, IT proficiency, and reporting assessment that have not been studied in prior studies while our research model does not control for variables already known to influence insiders' intention to disclose.

2.1 Privacy and compliance in healthcare

Privacy is considered as one of the key relational principles between patients and physicians. To receive quality healthcare, patients need to share their health information with their physicians. This personal health information is sensitive. Disclosing this information may negatively affect patients' lives. Regulations such as HIPAA were established to protect patients' privacy and confidentiality. HIPAA includes security and privacy components for healthcare professionals to comply with. The security component stipulates methods necessary to protect patient information while the privacy component handles the issues of limitation, responsibility, and access control. As to compliance with these regulations, its responsibility falls on individual healthcare providers. While acknowledging the significance of protecting health information security, prior studies have investigated behaviors of health information disclosing, predictors, and outcomes as shown in Table 1. Prior studies consistently show that personal factors play a significant role in the context of health information disclosing behaviors. For example, individuals' agreeableness and emotional instability positively influence their health information sensitivity in the context of web-based healthcare services [18]. In particular individuals' negative emotional status caused by their current medical state increases their disclosing of health information [19]. Similarly, student nurses' personal factors (e.g., personal norms, self-control) are likely to impact their health information disclosing behaviors in hospitals [4]. However, student nurses' collectivistic tendency and IT proficiency, which are important virtues for accomplishing the healthcare profession [16], have been under-investigated. Investigating these can provide researchers and practitioners with valuable insights into HISA education.

Table 1 Literature review on health information disclosing behaviors

Study	Predictors	Dependent variable	Findings
Bansal and Gefen [18]	• Perceived health information sensitivity • Personality (agreeableness and emotional instability) • Health information privacy concern • Trust in health website • Previous online privacy invasion • Risk beliefs • Prior positive experience with the website, etc	• Intention to disclose health information	• Negative influence of health information privacy concern on intention to disclose • Positive impacts of prior positive experience with the website on trust in the website and intention to disclose • Positive influences of perceived health information sensitivity and previous online privacy invasion on health information privacy concern
Anderson and Agarwal [19]	• Cognitive factors (electronic health information privacy concern, trust in electronic medium) • Health status emotion • Risk scenario variables (intended purpose, requesting stakeholder)	• Willingness to provide access to personal health information	• Significant moderating roles of intended purpose and requesting stakeholder between the cognitive factors and willingness to provide access • Negative impact of negative emotion on willingness to provide access
Jin [20]	• Behavioral activation systems • E-health website evaluation • Prevention regulatory focus •Self-concealment tendency, etc	• Truthful disclose • Information withholding • Information sensitivity	• Negative impact of truthful disclosure on information withholding • Positive impact of e-health website evaluation on truthful disclosure • Positive impact of self-concealment tendency on information sensitivity
Park et al. [4]	• Health information security awareness (HISA) • Personal norms • Self-control	• Intention to disclose patient's health information	• Negative impacts of personal norms and self-control on disclosing intention
Park et al. [21]	• HISA • Medical assessment of patient's medical status	• Intention to disclose patient's health information	• Positive impact of HISA on intention to disclose patient's health information • Positive impact of medical assessment to disclosing intention
Esmaeilzadeh [22]	• Perceived transparency of privacy statement • Cognitive trust in health information exchanges (HIE)'s competency and integrity • Emotional trust in HIE	• Patient's information disclose intention	• Positive influences of cognitive trust in HIE's competency and integrity on emotional trust in HIE • Positive influence of emotional trust in HIE on disclosing intention

2.2 Deterrence theory and security awareness program approach

Deterrence theory is used to explain the rationale of deviant security behaviors and to suggest countermeasures to deter the behaviors [e.g., 23–27]. The theory views people capable of making decisions on whether they commit or abstain from a crime based on the analysis of cost and benefit [28]. It further suggests that people are more likely to abstain from deviant behaviors as perceived swiftness, certainty, and severity of punishment increase. The theory accentuates the vital role of sanctions in deviant security behaviors.

Prior studies investigate the countermeasures to deterrence theory. Straub and Welke [23] suggest training as an essential security countermeasure. D'Arcy et al. [27] find that the perceived severity of sanctions developed by education, training and awareness programs can deter information systems (IS) misuse intentions. Karjalainen and Siponen's [29] literature review on IS security organizes several security training approaches including the 'security awareness program' approach of interest in this study. With this approach, employees learn the significance of IS security and are trained to achieve IS security awareness, thus facilitating security compliance while dissuading deviant behaviors. IT training in nursing education should help student nurses develop an awareness of health information security [4].

Deterrence theory and subsequent studies on the security awareness program approach provide the theoretical basis for the development of our research model and hypotheses (see Fig. 1).

2.3 Health information security awareness

Health information security awareness (HISA) refers to the overall knowledge of general information security, health information security, and relevant regulations and punishments that can be achieved [4]. The concept of HISA is developed based on prior studies suggesting that security education, training, and awareness programs can discourage individuals' deviant security behaviors [27, 29]. Three types of awareness construct the HISA: (1) general information security awareness, (2) health information security regulation awareness, and (3) punishment severity awareness. Nursing curricula develop student nurses' awareness of health information security in classes as well as hospital awareness programs and orientations [4].

General information security awareness indicates general knowledge of health information security issues and their significance [4]. A non-healthcare context study found that employees' awareness of general information security positively affects their attitude toward information security policy compliance [30]. Students can achieve their general information security awareness in course lectures and hospital-based awareness programs.

The concept of *health information security regulation awareness* focuses on health care contexts [30]. This concept is defined as knowledge of health information security regulations and their requirements, for example, HIPAA. Violations of those regulations are administered in courts, while noncompliance with security policies is addressed within companies and organizations [31]. Student nurses can acquire their health information security regulation awareness by learning the history, principles, and requirements of the regulations.

Punishment severity awareness is defined as knowledge of the types and severity of sanctions in health information

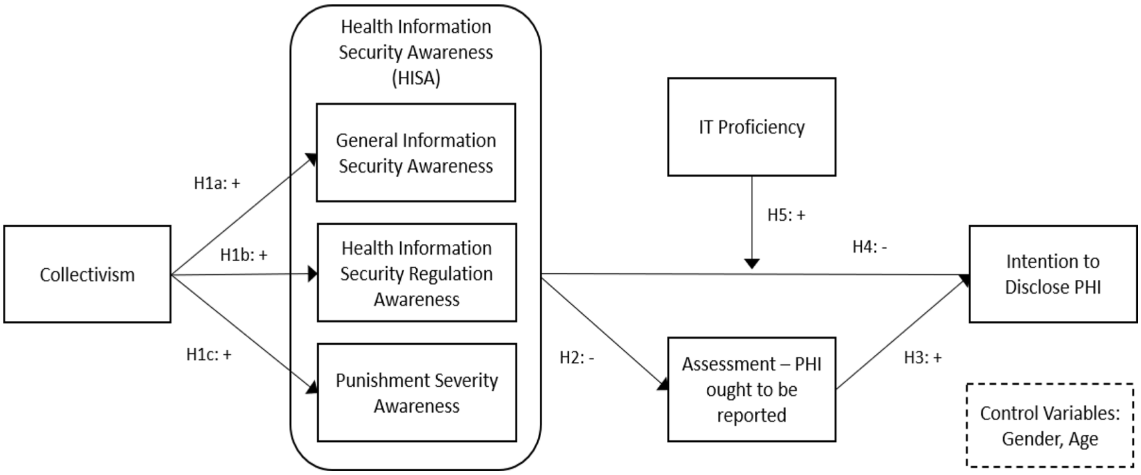
Health Information Security Awareness (HISA)
General Information Security Awareness
Health Information Security Regulation Awareness
Punishment Severity Awareness
Collectivism
H1a: +
H1b: +
H1c: +
IT Proficiency
H5: +
H4: -
Intention to Disclose PHI
H2: -
Assessment – PHI ought to be reported
H3: +
Control Variables: Gender, Age

Fig. 1 Research model

security violations [4]. It is important to note that compared with violations of policies in companies, the severity of punishments in violations of health information security laws can be much higher because relevant laws prescribe more severe sanctions [31]. This content is addressed in nursing curricula.

Prior studies report that HISA has positive relationships with individual characteristics such as personal norms, self-control [4], and self-efficacy to comply with policy [21]. HISA is also found to negatively influence individuals' medical assessment of patient's medical status and intentions to disclose patient's health information [21]. Further, HISA has positive impacts on the components of patient's health information protection awareness: that is, communication, management and referral [32].

Predictors of various security awareness have been reported by prior studies. Information richness (e.g., hypermedia-based and multimedia-based information) affects users' security awareness [33]. In addition, facilitating conditions (e.g., technical/organizational infrastructures) may positively influence the awareness of information security policy [34]. Finally, organizational factors (e.g., transformational leadership, information security culture) and individual factors (e.g., information system knowledge, negative experience) affect information security awareness [35, 36]. However, the predictors of HISA in the context of healthcare and nursing students have not, to our knowledge, been previously investigated. In this study, we particularly investigate collectivism as a predictor of HISA. The nursing profession focuses on the care of other individuals and public health, not the care of self. The Code also stipulates this collectivistic nature as an unchallengeable ethical standard in nurses' work settings [13]. Investigating the relationship between collectivism and HISA can offer insights on how to improve HISA for security compliance.

2.4 Collectivism and health information security awareness

Collectivism refers to normative standards, in which an individual believes that "collective or group interests should take precedence over individual self-interest" [16, p. 5]. Collectivistic value, a personality characteristic of value [37], means normative standards that impact an individual's choice on the various courses of action the s/he perceives [37]. Some studies use the concept of collectivism in between-culture contexts and consider it one of the leading characteristics that can distinguish from native cultures [38, 39]. In contrast, other studies use collectivism value in within-culture contexts where individuals cooperate in collective, group, or organizational settings and investigate individual's collectivistic tendency [37, 40–42]. Our study subscribes to the latter research stream on collectivism.

Our study chooses collectivism and focuses its relationship with HISA. According to the Office for Civil Rights [7], student nurses are prescribed as patient care providers during their practical training. They should internalize the values of the Code because the Code stipulates non-negotiable ethical standards and obligations of nurses [14, 15]. The Code highlights the nurse's primary commitment to collective wellbeing. For example, provisions six and nine emphasize the nurse's obligations on a collective effort to maintain the ethical environment and integrity of the profession [14, 15]. Provision three highlights the nurse's obligations to protect patients' rights. Winland-Brown et al. [14] further interpret provision three to emphasize the duties of protecting patient's privacy and confidentiality. The collectivism level patient care providers have can be crucial for patient care during healthcare crises. For instance, during the COVID-19 pandemic, healthcare workers with a high level of collectivism tend to sacrifice their self-interests for collective wellbeing [43].

Prior studies suggest that individuals with high collectivistic values are more likely to subordinate self-interests over organizational interests and engage in socially cooperative behaviors while being aware of organizational needs [16, 42]. Also, such individuals are more likely to partake in prosocial behaviors, which help others at their own cost [44]. Student nurses take content-specific training as a part of their course curriculum, which leads them to achieve general information security awareness [4, 45]. Specially, they need to take such courses (e.g., introduction of management information systems, nursing management), in which they learn general information security, basic concepts of health records, security, threats, and impacts [4]. Since student nurses highly value collective goods, they tend to expose themselves to a broader scope of information (including security) instead of limited information for their committed tasks [37]. Thus, we argue that student nurses who have a high level of collectivistic values and norms are likely to have a high awareness of general information security. They tend to have strong interests in learning general health information security, relevant threats, and impacts. Therefore, we hypothesize that:

H1a Collectivism is positively associated with general information security awareness.

A prior study suggests that individuals with high collectivistic values try to conform to their societies, focusing on achieving collective goods and maintaining their faces [46]. To achieve conformity with their societies, individuals need to know what others expect them to do represented in laws and regulations [37]. To learn health information security regulations, student nurses take courses on health care laws and regulations. Similarly, they learn health care regulations and policies during clinical training at hospitals. Thus, student nurses with high collectivistic values are more likely to learn health care regulations. Therefore, we hypothesize that:

H1b Collectivism is positively associated with health information security regulation awareness.

A prior study suggests that individuals with high collectivistic values tend to behave prosocially toward members in social circles to avoid punishment [44]. Societies typically monitor individuals' illegal behaviors and punish nonconformity. Monitoring and punishment play critical regulating roles in social relationships [44]. Thus, individuals with high collectivistic values try to avoid situations where they do not conform to collective norms. In the same vein, student nurses learn relevant punishments and the level of severity for nonconformity by taking nursing courses in school and clinical training at hospitals [4]. Student nurses who have high collectivistic values are more likely to make an effort to learn the types of punishments associated with different levels of breaches of health information security. They do this to conform to collective norms and regulations. Therefore we hypothesize that:

H1c Collectivism is positively associated with punishment severity awareness.

2.5 Health information security awareness and reporting assessment

The concept of whether or not PHI (e.g., patient's medical status) should be reported originates from whistleblowing research [47–49]. Student nurses must determine whether a patient's medical status ought to be reported to relevant parties. They are taught the significance of health information security, the impact of the security breach, and the sanctions prescribed in regulations. Additionally, they learn the importance of communication and collaboration with family inscribed in the Code. Winland-Brown et al. [14, p. 270] point out that "nurses must address conflicting expectations from patients, families, and physicians, as well as conflicts arising between their own professional and personal values."

When family members of a patient ask for the patient's medical status, student nurses may face the conflict of whether the patient's medical status ought to be reported. Park et al. [49] suggest that when people face a problem, they assess if the status of the problem needs to be reported and contemplate if they are responsible for reporting. The assessment ultimately impacts their willingness to report. As student nurses' HISA increases they are less likely to determine that the patient's medical status ought to be reported. A prior study finds a direct negative relationship between HISA and medical assessment-patient's medical status, with the presence of a mediator (i.e., self-efficacy to comply) [21]. Different from the prior study, with the presence of a predictor (i.e., collectivism) and a moderator (IT proficiency), we hypothesize that:

H2 HISA is negatively associated with a student nurse's assessment that s(he) should report PHI.

2.6 Reporting assessment, health information security awareness, and intention to disclose PHI

Whistleblowing literature suggests that once people observe wrongdoing, they assess the seriousness of the situation, the parties that committed the act, and the cost/benefit of whistleblowing [e.g., 47, 50]. The literature also suggests that people tend to blow the whistle when they assess that the wrongdoing and harm are serious, the benefit of whistleblowing outweighs the cost, and they feel their responsibilities to report [50]. Then, people tend to blow the whistle of organizational wrongdoings. In the context of IT projects, Park et al. [50] found that employees were willing to communicate bad news in troubled IT projects to relevant stakeholders. Similarly, a prior study reports that student nurses are more likely to have intentions to disclose patient's medical status to family members when they assess the situation as a serious status that requires communication with family and that ought to be reported [21]. Again, different from this study [21], with the presence of collectivism and IT proficiency, we examine this relationship to see whether the findings are consistent in the present study. Thus, we hypothesize that:

H3 A student nurse's reporting assessment that PHI should be reported is positively associated with an intention to disclose PHI.

In the context of student nurses, prior studies show mixed results on the relationship between HISA and disclosing intention. A study reports a direct negative relationship between them [21]. However, another study finds an indirect relationship [4] between them: that is, with the presence of the mediators (i.e., personal norms and self-control), HISA reduces disclosing intentions [4]. In this study, we propose a direct relationship between HISA and disclosing intentions without the mediators. A prior study suggests that security countermeasures such as security policy, SETA program, and computer monitoring increase the perceived severity of sanctions, and in turn, the perception of sanction severity decreases IS misuse intention [27]. In the security compliance context, other studies particularly focus on examining the role of 'awareness' of information security, policies and their requirements, and punishments of security breaches through security education programs [27, 51]. They find that deviant security behaviors of employees can be discouraged by enhancing such awareness. Additionally, awareness of information security policy is found to increases policy compliance attitude [30]. Based on these findings, we argue that student nurses who have a high awareness of health information security, regulations, and severity of punishments are less likely to disclose PHI [21]. Thus, we hypothesize that:

H4 HISA is negatively associated with intention to disclose PHI.

2.7 Moderating role of IT proficiency on health information security awareness and intention to disclose PHI

Prior studies on security policy compliance in the organization contexts identify various moderators. For example, perceived sanction certainty and neutralization (via a denial of the victim and metaphor of the ledger) are found to moderate the relationship between perception of procedural injustice and intention to commit employee computer abuse [52]. Information security policy (ISP)-related ascription of personal responsibility moderates the relationship between ISR-related personal norms and ISP compliance behavior [53]. Rules-oriented ethical climate and susceptibility to interpersonal influence are reported to moderate the relationship between self-regulatory approach and ISP compliance [53].

Because of the nature of the healthcare context where patient care providers operate sophisticated medical technologies to support medical procedures and use IT to process electronic medical records for delivering administrative services, improving IT proficiency is a critical task for student nurses to provide quality services [54]. Despite the significance of IT proficiency, the moderating role of IT proficiency in the relationship between HISA and intention to disclose PHI has not, to our knowledge, been previously examined.

IT proficiency refers to the mastery level of technical knowledge and skills needed to fulfill one’s job responsibilities [17]. A prior study [55] suggests that individuals with a low level of IT proficiency have a basic understanding of IT and security-related hardware/software components. On the other hand, ones with a high level of IT proficiency can apply their understanding and knowledge of information security to security practices as well as guide others to comply with policy and regulation. Thus, this implies that the negative relationship between HISA and disclosing intention may be contingent on IT proficiency. Compared with student nurses with a low level of IT proficiency, student nurses with a high level of IT proficiency may be more aware of the significance of information security as well as relevant security policy and regulation, thereby being less willing to disclose PHI. Thus, we hypothesize that:

H5 IT proficiency strengthens the negative relationship between HISA and intention to disclose PHI.

3 Research methodology

A survey method was employed to collect data. Partial Least Square (PLS) was used to analyze collected data and examine our research model. We first compared the means and standard errors of the measurement items. We then used partial least squares (PLS) analysis of the structural model using SmartPLS 3.2. Considering the explorative nature of this study, we chose PLS which can reduce the risk of omitted variable bias. However, we do not claim that PLS can fully mitigate the risk. Following standard procedures, we first assessed the measurement model and then the structural relationships. This study adopted measurement items used by prior information security studies to collect data about student nurses' intent to disclose PHI. The constructs, measurement items, and information sources used in our study were shown in “Appendix A”.

3.1 Subjects

The subjects were nursing students who enrolled in nursing courses at a large urban university in the US. In our study, student nurses represent a weak security link instead of regular nurses at healthcare organizations. After receiving institutional IRB approval, all students enrolled in a pre-licensure undergraduate nursing program were asked to participate in the online survey. The survey questionnaires were set up on the SurveyMonkey site. Subjects received a scenario in which a patient was diagnosed with a disease such as flu. Then, the subjects were asked to answer questions on their behavioral intentions and perceptions shown in “Appendix A”.

3.2 Data collection

One hundred ten students voluntarily participated in the online survey. Due to the incomplete and inconsistent data input, five subjects were dropped. A total of 105 usable data points was collected. The subjects comprised 20 males and 85 females. Additional demographic details are shown in Table 2. No identification was collected to ensure anonymous data collection and to reduce common method bias [56]. Anonymous data collection reduces subjects’ tendency to provide answers that are socially desirable or best meet the researchers’ expectations. In addition, we adopted measures that had been previously validated in the literature.

Table 2 Demographic details

	Category	#		Category	#
Age	15–20	12	Semester	1	18
	21–25	40		2	11
	26–30	25		3	5
	31–35	11		4	23
	36–40	7		5	17
	41–45	4		6	11
	Over 46	6		7	19
				8	1

4 Results

4.1 Method of data analysis

The research model is multistage which requires structural equation modeling and simultaneously tests multiple relationships. Statistical tools used to analyze the data included SPSS and SmartPLS. SPSS was used to conduct a basic analysis of the collected data, including a test for item normality, means, and outliers. PLS was used to examine the magnitude of the relationships and the effects between the constructs in our model [57]. For validating measurement and for evaluating the hypothesized paths in the research model, SmartPLS 3.2 software was used [58]. PLS is appropriate for testing a complex model that includes formative constructs and mediation [59–61] and is useful for maximizing the explained variance of any endogenous variables in the structural model [62]. Focusing on theory development, our study is explorative. PLS is known to be suitable for predicting theoretical models in their early stages such as ours [61]. Compared with covariance-based SEM and MANOVA, PLS with strong statistical power enables researchers to capture statistically significant relationships even with a small sample size [63]. In addition, PLS enables researchers to lead to accurate and insightful findings because it minimizes the effects of omitted variable bias and examines structural paths among variables [64]. Compared with regression, PLS is well-suited to evaluate a model with multidimensional second-order constructs such as HISA [65]. Following standard procedures, we first assessed the measurement model and then the structural relationships.

4.2 Ensuring reliability and validity

Two pilots were conducted to test our survey instrument. As a result of both pilot tests, the instrument was refined. Reliability was assessed by checking Cronbach's alpha, composite reliability, and the average variance extracted (AVE). Research recommends a Cronbach's alpha score of 0.70 as extensive evidence of reliability and 0.80 or higher as exemplary evidence [66]. All constructs in the measurement model exhibited Cronbach's alpha of 0.735 or higher, and composite reliability of 0.867 or higher (see Table 3). As to collectivism, we used four measurement items adapted from [37]. Two items among them were dropped due to low loading scores. All the AVEs exceeded the acceptable level of 0.5 or higher [67].

Table 3 Item loadings and construct reliability

Construct	Item	Standardized loading	Cronbach's Alpha	Composite reliability	AVE
Collectivism	CO1	0.963	0.735	0.867	0.767
	CO2	0.779			
Security awareness	RA1	0.952	0.878	0.924	0.803
	RA2	0.807			
	RA3	0.922			
Rule awareness	RA1	0.982	0.979	0.986	0.959
	RA2	0.983			
	RA3	0.973			
Penalty severity awareness	PA1	0.919	0.923	0.951	0.866
	PA2	0.949			
	PA3	0.924			
Reporting assessment	MA1	0.928	0.837	0.901	0.753
	MA2	0.782			
	MA3	0.887			
Intention to disclose	ID1	0.927	0.931	0.956	0.879
	ID2	0.953			
	ID3	0.931			

Discriminant validity was assessed. Each indicator's loading was calculated on its construct and its cross-loading on all other constructs (see "Appendix B"). Analysis showed that the former is higher than the latter. Therefore, the psychometric adequacy of our measurement model was established. We compared AVE for each reflective construct with the shared variance between all possible pairs of reflective constructs to check discriminant validity (shown in "Appendix C"). The AVE for each construct was higher than the squared correlation between the construct pairs. Therefore, discriminant validity was established. This result indicated that the latent construct and its block of indicators shared more variance than the latent construct and its block of indicators did. The correlations among all constructs are below the 0.90 threshold, which suggests that all constructs are distinct from each other, as shown in Table 4.

Standardized loadings were examined to check the convergent validity of constructs. To satisfy the condition that the shared variance between each item and its associated construct exceeds the error variance, standardized loadings should be larger than 0.707 [67]. All loadings were larger than 0.782 (see Table 3).

4.3 Common method variance (CMV)

To test the threat of CMV, we conducted Harman's one-factor test [56]. We examined whether a single factor accounted for a significant proportion of the variance. The single factor would emerge if there is a CMV. Harman's one-factor test showed that no such factor emerged. We loaded all items, both independent and dependent variables, into a single exploratory factor analysis. The analysis showed three factors with eigenvalues higher than 1. Taken together, these factors explained 60.1% of the variance of the data, with the first extracted factor accounting for 29.9% of the variance in the data. Given that three factors were extracted from the analysis, and that the first factor accounted for less than 50% of the variance, this suggests that CMV is unlikely to be a significant issue. In addition, we addressed social desirability which could be a possible source of CMV [68]. Ambiguous questions and negative words in questionnaires may cause subjects to choose socially desirable answers. Our questionnaire's flesch-kincaid reading level is 9.4 and does not contain many negative words which might have a significant impact on the measurement model. Therefore social desirability bias was not an issue in our study.

4.4 Structural model

To test our hypotheses, we examined the path coefficients, significance level, and R^2 values in the structural model. The path coefficients indicate the relationship strength between two constructs, while R^2 denotes the amount of variance [69]. The R^2 value for the dependent variable (Intention to Disclose) was 0.49. This value indicates that the research model accounts for 49% of the variance in the dependent variable. We also reviewed the R^2 values for similar constructs in other studies. The R^2 of 0.49 for the dependent variable is comparable to results reported by prior studies and shows strong evidence of the explanatory power of our research model.

The path coefficients in the structural model were calculated with the entire sample. To obtain the t-values corresponding to each path (shown in Fig. 2), we employed the bootstrapping method with 500 resamples. At the significance levels of 0.05 and 0.01, acceptable t-values for two-tailed tests are 1.96 and 2.58 respectably. Five of seven hypotheses were supported, as shown in Table 5.

Moderators refer to variables that influence the strength or direction of a relationship between an independent variable and a dependent variable. First, the impact of IT proficiency on the strength of the relationship between HISA and Intention to Disclose can be seen by examining the explained variance. The slight increase of R^2 from 0.42 to 0.49 does not show a strong influence of the moderator on the strength of the relationship. Second, moderation of the direction of the relationship is detected by looking at the interaction effects. The significant regression coefficient for the interaction terms (with a path coefficient of −1.34 which is significant at 0.01 level) indicates IT Proficiency negatively impacts the relationship between HISA and Intention to Disclose.

Table 4 Correlation among constructs

Measure	1	2	3	4	5	6
Collectivism	–					
Security Awareness	0.115	–				
Rule Awareness	0.164	0.461**	–			
Penalty Awareness	0.209*	0.359**	0.465**	–		
Reporting Assessment	0.141	−0.251**	−0.251**	−0.099	–	
Intention to Disclose	−0.106	−0.423**	−0.432**	−0.517**	0.331**	–

*Significant correlations at $p < 0.05$ level, **significant correlations at $p < 0.01$ level

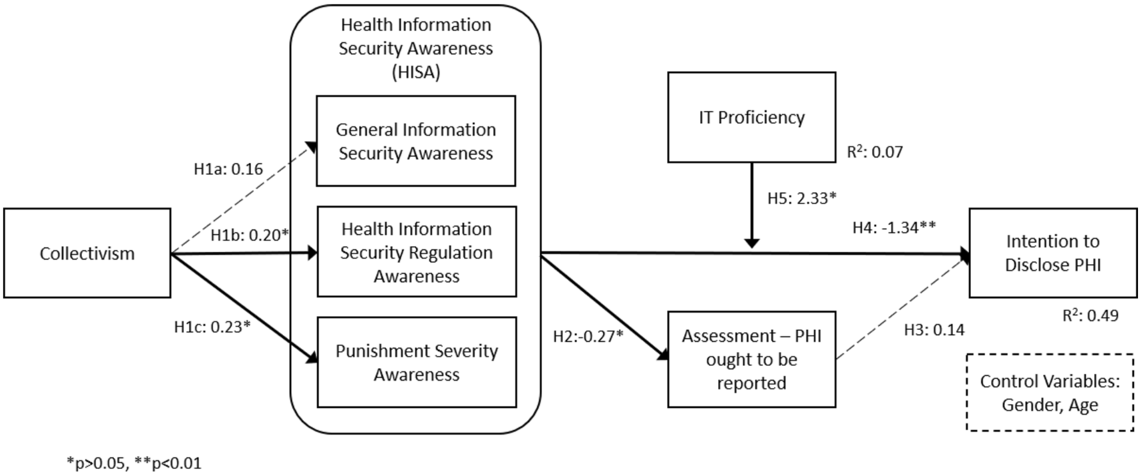
Health Information Security Awareness (HISA)
General Information Security Awareness
Health Information Security Regulation Awareness
Punishment Severity Awareness
Collectivism
H1a: 0.16
H1b: 0.20*
H1c: 0.23*
IT Proficiency
R^2: 0.07
H5: 2.33*
H4: -1.34**
Intention to Disclose PHI
R^2: 0.49
H2:-0.27*
Assessment – PHI ought to be reported
H3: 0.14
Control Variables: Gender, Age
*p>0.05, **p<0.01

Fig. 2 Results of PLS analysis. *Note* Solid line indicates a significant; Dotted line indicates a non-significant relationship

Table 5 Results of hypotheses test

Hypothesis	Explanation	Result
H1a	Collectivism increases general information security awareness (β = 0.16, p > 0.05). Prior studies [16, 42] suggest that individuals with high collectivism values tend to prioritize organizational interests over self-interests. As a result, they are socially cooperative and help others in their organizations. To our knowledge, our study is a first attempt to examine this relationship. The positive relationship between collectivism and great information security awareness is not supported	Unsupported
H1b	Collectivism increases health information security regulation awareness (β = 0.20, p < 0.05). The same assumption mentioned above applies to this relationship [16, 42]. Our study is, to our knowledge, a first attempt to test this relationship. The finding suggests that high collectivism is more likely to lead to greater information security regulation awareness	Supported
H1c	Collectivism increases punishment severity awareness (β = 0.23, p < 0.05). The same assumption mentioned above applies to the relationship [16, 42]. Again, the present study is a first attempt to examine this relation. The result suggests that high collectivism is more likely to lead to a greater punishment severity awareness	Supported
H2	*HISA decreases a student nurse's reporting assessment that PHI ought to be reported* (β = – 0.27, p < 0.01). A prior study reports a direct negative relationship between HISA and medical assessment-patient's medical status, with the presence of a mediator (i.e., self-efficacy to comply) [21]. Differ from the prior study, with the presence of a predictor (i.e., collectivism) and a moderator (IT proficiency), our findings suggest that a high HISA is more likely to lead to the reporting assessment that a PHI ought to be reported	Supported
H3	*A student nurse's reporting assessment that PHI ought to be reported increases intention to disclose PHI* (β = 0.14, p > 0.05). Whistleblowing literature suggests that individuals are more likely to blow the whistle when they assess that the wrongdoing and harm are serious, the benefit of whistleblowing outweighs the cost, and they feel a responsibility to report [50]. Based on the assumption, our study adapted the constructs and tested in a different context, health information security compliance. A prior study finds a significant negative relationship between reporting assessment and disclosing intention, with the presence of a mediator (self-efficacy to comply) [21]. Different from this study [21], with the presence of collectivism and IT proficiency, we examine this relationship, but the assumption does not hold in the relationship between the reporting assessment and disclosing PHI	Unsupported
H4	HISA decreases intentions to disclose PHI (β = – 1.34, p < 0.01). Prior study [4] finds a non-significant relationship between HISA and disclosing intention when individual characteristics of personal norms and social-control are examined together. In contrast, our result shows a significant direct relationship between HISA and disclosing intention, suggesting that individuals with high HISA are less likely to disclose PHI	Supported
H5	IT proficiency strengthens the negative relationship between HISA and intention to disclose PHI (β = 2.33, p < 0.05). Prior study [55] suggests that individuals with a high level of IT proficiency can apply their understanding and knowledge of information security to security practices and guide others to comply with policy and regulation. Based on this assumption, this study examines the moderating role of IT proficiency in the relationship between HISA and disclosing intention, which is, to our knowledge, a first attempt to investigate this relation. Our finding implies that as the level of IT proficiency increases, the negative effect of HISA on intention to disclose PHI increases as well	Supported

5 Discussion

The purpose of this study is to theoretically explain health information disclosing intentions of student nurses by exploring antecedent factors (i.e., collectivism, HISA, reporting assessment, and IT proficiency) to disclosing intentions. We develop and empirically test a research model which does not control for variables known to affect intention to disclose from prior research.

5.1 Implications for research

The Code emphasizes the importance of collectivistic values for nursing professionals, particularly protecting patient's privacy and confidentiality [13–15]. Despite the significance, we found no studies that investigated the relationship between student nurses' collectivistic value and HISA. This study contributes to medical informatics, nursing education, and information security literature by finding that the collectivistic values may significantly influence the two components of HISA—health information security regulation awareness and punishment severity awareness (H1b and H1c). Our study offers a nuanced understanding of the relationships between collectivistic value and each HISA component. People with high collectivistic values are more likely to have a high awareness of security regulations and high awareness of punishment severity. Our results show that this does not mean that people with high collectivistic values would have high general information security awareness such as overall costs of potential security issues. Thus, employees with high collectivistic values may not automatically translate into that they have a high level of general information security awareness. When nursing schools and healthcare organizations educate healthcare providers including student nurses, they should focus on the general security management including cost/benefit analysis of security issues.

Our findings are consistent with a prior study, with the presence of a mediator (self-efficacy to comply), that shows the negative impact of HISA on reporting assessment and on disclosing intention [21]. Our study is different from the prior study in that these relationships are examined with the presence of a predictor (i.e., collectivism) and a moderator (IT proficiency). Our findings suggest that student nurses weigh the cost and benefit between 'not disclosing PHI,' which originated from HISA, and 'disclosing PHI,' which might stem from the understanding of the significance of communication and collaboration with family. Our results show that student nurses with high HISA are less likely to assess that PHI should be reported (H2 and H4). However, different from the prior study [21], reporting assessment does not have a significant impact on intention to disclose (H3). A significant implication from the findings is that HISA rather than reporting assessment plays a critical role in affecting intention to disclose PHI. These findings are also consistent with prior information security literature [23, 29] in that education and training help employees achieve security awareness.

We adapted the measurement items for the reporting assessment, which were originally developed in the context of whistleblowing literature [49]. Our study shows that such adapted measurement items are applicable not only in the whistleblowing context but also in security compliance in the context of health information security. Future studies using the adapted items can identify other factors relevant to reporting assessment.

Prior studies have suggested that IT proficiency is an individual's essential ability to protect information security [55, 70]. Especially, in healthcare contexts where patient care providers use IT to process electronic medical records and to support medical procedures, enhancing IT proficiency is very important for student nurses [54]. Despite its importance, the role and the impact of IT proficiency in disclosing behaviors have been under investigated. Our study is the first attempt to investigate the role of IT proficiency in the context of student nurses' disclosing behaviors (H5). The findings suggest that IT proficiency plays a moderating role in the relationship between HISA and intention to disclose PHI. Thus, when student nurses have high IT proficiency, the negative impact of HISA on the disclosing intention is strengthened. The results provide significant implications and suggest that enhancing the IT proficiency of student nurses can be one of the essential security countermeasures to discourage disclosing intentions and behaviors.

Finally, prior studies report mixed results on the relationship between information security awareness and security policy compliance behaviors. Bulgurcu et al. suggest that information security awareness of employees in organizations positively affect their compliance with security policy [30]. On the other hand, Park et al. find no direct impact of student nurses' health information security awareness (HISA) on their disclosing intentions [4]. However, they note that student nurses' individual characteristics such as personal norms and self-control mediate the relationship between HISA and disclosing intentions. Specifically, HISA positively influences personal norms and self-control, which in turn negatively impact disclosing intentions [71]. In contrast, our study finds a significant positive relationship between HISA and intention to disclose, which is consistent with the findings of Park et al.'s subsequent study [21].

However, no statistically significant relationship between the reporting assessment and disclosing intention is found. This suggests no mediating role of the reporting assessment (H2 and H3). To our knowledge, this study is a first attempt to investigate the role of the reporting assessment in the context of disclosing intentions. Our study offers additional insights to nursing education and information security literature by finding that HISA reduces the reporting assessment and disclosing intentions when reporting assessment and IT proficiency are examined together.

5.2 Implications for practice

Collectivistic values are crucial in the nursing profession to establish, maintain and enhance a safe, ethical, and quality healthcare environment [14, 15]. The collectivistic nature can be an essential individual characteristic of nurses. These findings suggest that education should help student nurses internalize collectivistic values, which can positively impact each component of HISA thereby discouraging deviant security behaviors.

This study highlights the significance of enhancing the IT proficiency of student nurses to discourage their disclosing intentions. IT proficiency can bolster the dissuading impact of HISA on student nurses' disclosing intentions. Student nurses should achieve technical knowledge and skills that help them fulfill their responsibilities and duties at works. To support them, nursing schools and faculties should educate not only the basic components of IT but also security-related components (e.g., security constraints, relevant technology policies, consequences of violation). Consequences for violating policies are particularly significant in strengthening the discouraging impact of HISA on disclosing intentions.

5.3 Limitations and future research

In this study, we investigated student nurses' disclosing intentions. Collecting data on actual disclosing behaviors may be desirable, yet practically not feasible. However, many prior studies on security policy compliance report that intentions effectively predict actual abnormal security behaviors [e.g., 24, 72–74]. Although this study limits to a few variables to restrain extraneous variances, other factors might impact the disclosing intentions. For example, unsupported H3 might mean that other factors play between reporting assessment and intention to disclose. Factors such as responsibility and morality may work as mediators [49]. Future research is needed to further investigate other relevant factors (e.g., individual, organizational, work-related, and cultural factors). In addition, constructs other than IT proficiency can be a moderator between HISA and intention to disclose. Finding and testing those moderators can be done by future research.

Our study suggests that student nurses engage in the assessment of whether a patient's status should be reported or not. Further practical examination of whether the assessment involves cost and benefit analysis will be valuable. For instance, a prior study [30] finds that benefit of compliance, cost of compliance, and cost of noncompliance have significant relationships with security policy compliance. This may hold up in the healthcare context such as student nurses' disclosing intentions too.

Our data collection is limited to student nurses in one university. We did not explore whether our findings would be applicable to other medical professionals such as doctors. Therefore, our findings may not be generalizable. Our intention was not to generalize our findings, but rather to exploratively develop and test our research model. Our findings' generalizability to other medical team members can be examined by future study.

6 Conclusion

Insiders' security breach on patients' privacy is a serious concern for healthcare organizations. Our study aims to fill a research gap in understanding factors affecting insiders' intentions to disclose PHI. We identify and investigate factors (e.g., HISA, collectivism, reporting assessment, and IT proficiency) that may affect insiders' disclosing intentions. We find that collectivism affects two components of HISA, which then influences reporting assessment and disclosing intention. We also suggest that IT proficiency moderates the relationship between HISA and intention to disclose. Our study implies that we need to carefully consider individuals' collectivistic nature, HISA, and IT proficiency in reducing insiders' security breaches.

Appendix A: Measurement items and informing sources

Construct	Measurement items (1 = strongly disagree to 7 = strongly agree)	Borrowed/adapted	Informing sources
Intention to Disclose Protected Health Information (PHI)	• I may disclose the medical condition of the patient to the spouse. (mean: 1.67, std.dev: 1.09) • I intend to disclose the medical condition of the patient to the spouse. (mean: 1.50, std.dev: 0.89) • I expect to disclose the medical condition of the patient to the spouse. (mean: 1.60, std.dev: 1.04)	Borrowed	[4, 30, 75]
Collectivism	•Group success is more important than individual success. (mean: 4.78, std.dev: 1.64) • Being loyal to a group is more important than individual gain. (mean: 4.82, std.dev: 1.63)	Borrowed	[37]
General Information Security Awareness	• Overall, I am aware of the potential and general security threats and their negative consequences. (mean: 6.25, std.dev: 0.86) • I have sufficient knowledge about the cost of potential and general security problems. (mean: 5.77, std.dev: 1.46) •I understand the concerns regarding information security and the risks they pose in general. (mean: 6.28, std.dev: 0.88)	Borrowed	[4, 30]
Health Information Security Regulation Awareness	• I know the rules and regulations for the protection of PHI. (mean: 6.21, std.dev: 1.03) • I understand the rules and regulations for the protection of PHI. (mean: 6.25, std.dev: 1.03) • I know my responsibilities as prescribed in the rules and regulations for the protection of PHI. (mean: 6.16, std.dev: 1.14)	Borrowed	[4, 30]

Construct	Measurement items (1 = strongly disagree to 7 = strongly agree)	Borrowed/adapted	Informing sources
Punishment Severity Awareness	• I am aware that nurses who break health information security rules would be disciplined. (mean: 6.40, std.dev: 0.96) • I am aware that nurses who repeatedly break health information security rules may be laid off. (mean: 6.55, std.dev: 0.72) • If I were caught violating health information security rules/regulations, I would be severely punished. (mean: 6.35, std.dev: 0.89)	Modified	[24, 75, 76]

Construct	Measurement items (1 = strongly disagree to 7 = strongly agree)	Borrowed/adapted	Informing sources
Assessment-PHI Ought to be Reported	• I believe that something should be done to make the patient's medical test result known to the spouse. (mean: 2.73, std.dev: 1.87) • I believe that it really matters whether the patient's medical test result is made known to the spouse. (mean: 3.32, std.dev: 1.91) • Even if it is not me, I believe that someone should tell the spouse about the patient's medical test result. (mean: 2.82, std.dev: 1.85)	Modified	[49]
IT Proficiency	• Please choose your proficiency in using information technology in general (e.g., computer) (1 = novice to 7 = expert). (mean: 4.43, std.dev: 1.32)	Modified	[17]

Appendix B: Factor loadings

	1	2	3	4	5	6
Collectivism 1	**0.963**	0.188	0.223	0.236	0.075	−0.145
Collectivism 2	**0.780**	0.047	0.069	0.149	0.137	−0.048

	1	2	3	4	5	6
Security Awareness 1	0.143	**0.952**	0.480	0.481	−0.259	−0.430
Security Awareness 2	0.079	**0.807**	0.300	0.169	−0.228	−0.291
Security Awareness 3	0.190	**0.922**	0.532	0.447	−0.225	−0.457
Rule Awareness 1	0.177	0.518	**0.982**	0.490	−0.270	−0.432
Rule Awareness 2	0.218	0.497	**0.983**	0.436	−0.247	−0.449
Rule Awareness 3	0.177	0.462	**0.973**	0.480	−0.263	−0.382
Pen-Sev-Awareness 1	0.147	0.322	0.326	**0.919**	−0.064	−0.434
Pen-Sev-Awareness 2	0.252	0.444	0.490	**0.949**	−0.127	−0.541
Pen-Sev-Awareness 3	0.234	0.427	0.500	**0.924**	−0.116	−0.482
Medical Assessment 1	0.053	−0.226	−0.293	−0.098	**0.928**	0.344
Medical Assessment 2	0.227	−0.108	−0.123	−0.027	**0.782**	0.249
Medical Assessment 3	0.039	−0.320	−0.241	−0.147	**0.887**	0.272
Intention to Disclose 1	−0.101	−0.462	−0.484	−0.572	0.337	**0.927**
Intention to Disclose 2	−0.160	−0.395	−0.360	−0.486	0.323	**0.953**
Intention to Disclose 3	−0.094	−0.406	−0.365	−0.417	0.284	**0.931**

Bold text indicate that each indicator's loading on its construct

Appendix C: AVE versus squares of correlations between constructs

Measure	1	2	3	4	5	6
Collectivism	**0.767**					
Security Awareness	0.013	**0.803**				
Rule Awareness	0.027	0.213	**0.959**			
Pen-Sev-Awareness	0.044	0.129	0.216	**0.866**		
Reporting Assessment	0.020	0.063	0.063	0.010	**0.753**	
Intention to Disclose	0.011	0.179	0.187	0.267	0.110	**0.879**

Bold text indicate that AVE for each construct

Declarations

Conflict of interest The authors declare that they have no conflicts of interest.

Ethical approval All procedures performed in this study involving human participants were in accordance with the ethical standards of the institutional research committee and with the 1964 Helsinki Declaration and its later amendments or comparable ethical standards.

Informed consent Informed consent was obtained from all individual participants involved in the study.

References

1. Bansal G, Zahedi F, Gefen D (2010) The impact of personal dispositions on information sensitivity, privacy concern and trust in disclosing health information online. Decis Support Syst 49(2):138–150
2. Department_of_Health_and_Human_Services. Health Information Privacy Law and Policy. HealthIT.gov (2017)
3. Peters S (2009) 2009 CSI computer crime and security survey executive summary. Computer Security Institute, New York
4. Park E, Kim J, Park Y (2017) The role of information security learning and individual factors in disclosing patients' health information. Comput Secur 65:64–76
5. Cannon AA, Caldwell H (2016) HIPAA violations among nursing students: Teachable moment or terminal mistake—a case study. J Nurs Educ Pract 6(12):41–48
6. Thompson PE, Bell PL (2007) Potential student abuse of technology in the clinical setting. Nurse Educ 32(4):145–146
7. Wimberley P, Isaacson J, Walden D, Wiggins N, Miller R, Stacy A (2005) HIPAA and nursing education: how to teach in a paranoid health care environment. J Nurs Educ 44(11):489–492
8. Skiba DJ (2011) Nursing Education 2.0: the need for social media policies for schools of nursing. Nurs Educ Perspect 32(2):126–127
9. Song Y, Lee M, Jun Y, Lee Y, Cho J, Kwon M, Lim H (2016) Revision of the measurement tool for patients' health information protection awareness. Healthc Inform Res 22(3):206–216
10. Calhoun BC, Kiel JM, Morgan AA (2018) Health insurance portability and accountability act violations by physician assistant students: applying laws to clinical vignettes. J Physician Assist Educ 29(3):154–157
11. Westrick SJ (2016) Nursing students' use of electronic and social media: law, ethics, and e-professionalism. Nurs Educ Perspect 37(1):16–22
12. Erdil F, Korkmaz F (2009) Ethical problems observed by student nurses. Nurs Ethics 16(5):589–598
13. Epstein B, Turner M (2015) The nursing code of ethics: Its value, its history. Online J Issues Nurs
14. Winland-Brown J, Lachman VD, Swanson EOC (2015) The new 'code of ethics for nurses with interpretive statements'(2015): practical clinical application, Part I. Medsurg Nurs 24(4):268–271

15. Lachman VD, Swanson E, Winland-Brown J (2015) The new 'Code of Ethics for Nurses With Interpretive Statements' (2015): practical clinical application, part II. Medsurg Nurs 24(5):363–368
16. Van Dyne L, Vandewalle D, Kostova T, Latham ME, Cummings L (2000) Collectivism, propensity to trust and self-esteem as predictors of organizational citizenship in a non-work setting. J Organ Behav 21:3–23
17. McCoy C (2010) Perceived self-efficacy and technology proficiency in undergraduate college students. Comput Educ 55(4):1614–1617
18. Bansal G, Gefen D (2010) The impact of personal dispositions on information sensitivity, privacy concern and trust in disclosing health information online. Decis Support Syst 49(2):138–150
19. Anderson CL, Agarwal R (2011) The digitization of healthcare: boundary risks, emotion, and consumer willingness to disclose personal health information. Inf Syst Res 22(3):469–490
20. Jin S-AA (2012) "To disclose or not to disclose, that is the question": a structural equation modeling approach to communication privacy management in e-health. Comput Hum Behav 28(1):69–77
21. Park E, Kim J, Wiles LL, Park Y (2019) Factors affecting intention to disclose patients' health information. Comput Secur 87:1–13
22. Esmaeilzadeh P (2020) The impact of the privacy policy of health information exchange (HIE) on patients' information disclosure intention. Comput Secur 95:1–11
23. Straub DW, Welke RJ (1998) Coping with systems risk: security planning models for management decision making. MIS Q 22(4):441–469
24. Herath T, Rao HR (2009) Protection motivation and deterrence: a framework for security policy compliance in organisations. Eur J Inf Syst 18(2):106–125
25. Herath T, Rao HR (2009) Encouraging information security behaviors in organizations: role of penalties, pressures and perceived effectiveness. Decis Support Syst 47(2):154–165
26. Straub DW (1990) Effective IS security: an empirical study. Inf Syst Res 1(3):255–276
27. D'Arcy J, Hovav A, Galletta D (2009) User awareness of security countermeasures and its impact on information systems misuse: a deterrence approach. Inf Syst Res 20(1):79–98
28. D'Arcy J, Herath T (2011) A review and analysis of deterrence theory in the IS security literature: making sense of the disparate findings. Eur J Inf Syst 20(6):643–658
29. Karjalainen M, Siponen M (2011) Toward a new meta-theory for designing information systems (IS) security training approaches. J Assoc Inf Syst 12(8):518–555
30. Bulgurcu B, Cavusoglu H, Benbasat I (2010) Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. MIS Q 34(3):523–548
31. Whitman M, Mattord H (2011) Principles of information security. Cengage Learning, Boston
32. Adawiyah R, Hidayanto AN, Hapsari IC, Ibrahim RMS (2019) Identification of how health information security awareness (HISA) influence in Patient'Health information protection awareness (PHIPA). In: Proceedings in the 2019 5th international conference on computing engineering and design (ICCED). IEEE, pp 1–6
33. Shaw RS, Chen CC, Harris AL, Huang H-J (2009) The impact of information richness on information security awareness training effectiveness. Comput Educ 52(1):92–100
34. Bulgurcu B, Cavusoglu H, Benbasat I (2008) Analysis of perceived burden of compliance: the role of fairness, awareness, and facilitating conditions. In: Association of information systems SIGSEC workshop on information security & privacy (WISP 2008), Paris, France
35. Flores WR, Ekstedt M (2016) Shaping intention to resist social engineering through transformational leadership, information security culture and awareness. Comput Secur 59:26–44
36. Haeussinger F, Kranz J (2013) Information security awareness: its antecedents and mediating effects on security compliant behavior. In: Proceedings in the thirty fourth international conference on information systems (ICIS) Milan, pp 1–16
37. Ritchie WJ, Anthony WP, Rubens AJ (2004) Individual executive characteristics: explaining the divergence between perceptual and financial measures in nonprofit organizations. J Bus Ethics 53(3):267–281
38. Hofstede G (1980) Culture's consequences. Sage, Beverly Hills
39. Earley PC (1993) East meets West meets Mideast: further explorations of collectivistic and individualistic work groups. Acad Manag J 36(2):319–348
40. Chatman JA, Barsade SG (1995) Personality, organizational culture, and cooperation: evidence from a business simulation. Adm Sci Q 40(3):423–443
41. Cox TH, Lobel SA, McLeod PL (1991) Effects of ethnic group cultural differences on cooperative and competitive behavior on a group task. Acad Manag J 34(4):827–847
42. Moorman RH, Blakely GL (1995) Individualism-collectivism as an individual difference predictor of organizational citizenship behavior. J Organ Behav 16(2):127–142
43. Guan Y, Deng H, Zhou X (2020) Understanding the impact of the COVID-19 pandemic on career development: insights from cultural psychology. 119
44. Irwin K (2009) Prosocial behavior across cultures: the effects of institutional versus generalized trust. In: Altruism and prosocial behavior in groups. Emerald Group Publishing Limited, pp 165–198
45. Schmidt R (1995) Consciousness and foreign language learning: a tutorial on the role of attention and awareness in learning. In: Schmidt R (ed) Attention and awareness in foreign language learning. University of Hawaii, second language teaching & curriculum center, Honolulu, Hawaii, pp 1–63
46. Lalwani AK, Shrum L, Chiu C-Y (2009) Motivated response styles: the role of cultural values, regulatory focus, and self-consciousness in socially desirable responding. J Pers Soc Psychol 96(4):870–882
47. Dozier JB, Miceli MP (1985) Potential predictors of whistle-blowing: a prosocial behavior perspective. Acad Manag Rev 10(4):823–836
48. Smith HJ, Keil M, Depledg G (2001) Keeping mum as the project goes under: toward an explanatory model. J Manag Inf Syst 18(2):189–227
49. Park C, Keil M, Kim JW (2009) The effect of IT failure impact and personal morality on IT project reporting behavior. IEEE Trans Eng Manag 56(1):45–60
50. Gundlach MI, Douglas SC, Martinko MJ (2003) The decision to blow the whistle: a social information processing framework. Acad Manag Rev 28(1):107–123
51. Wybo MD, Straub DW (1989) Protecting organizational information resources. Inf Resour Manag J 2(4):1–16
52. Willison R, Warkentin M, Johnston AC (2018) Examining employee computer abuse intentions: insights from justice, deterrence and neutralization perspectives. Inf Syst J 28(2):266–293
53. Yazdanmehr A, Wang J, Yang Z (2020) Peers matter: the moderating role of social influence on information security policy compliance. Inf Syst J 30(5):791–844
54. Eley R, Fallon T, Soar J, Buikstra E, Hegney D (2008) Nurses' confidence and experience in using information technology. Aust J Adv Nurs 25(3):23–35

55. Evans K, Reeder F (2010) A human capital crisis in cybersecurity: technical proficiency matters. Center for Strategic & International Studies, Washington
56. Podsakoff PM, MacKenzie SB, Lee J, Podsakoff NP (2003) Common method biases in behavioral research: a critical review of the literature and recommended remedies. J Appl Psychol 88(5):879–903
57. Marcoulides GA, Saunders C (2006) PLS: a silver bullet? MIS Q 30(2):iii–ix
58. Ringle C, Wende S, Will A (2005) SmartPLS 2.0. SmartPLS, Hamburg, Germany
59. Diamantopoulos A, Winklhofer HM (2001) Index construction with formative indicators: an alternative to scale development. J Mark Res 38(2):269–277
60. Ringle C, Sarstedt M, Straub D (2012) A critical look at the use of PLS-SEM in MIS quarterly. MIS Q 36(1):iii–xiv
61. Lowry PB, Gaskin J (2014) Partial least squares (PLS) structural equation modeling (SEM) for building and testing behavioral causal theory: when to choose it and how to use it. IEEE Trans Prof Commun 57(2):123–146
62. Gefen D, Straub DW, Boudreau MC (2000) Structural equation modeling and regression: guidelines for research practice. Commun Assoc Inf Syst 4(1):1–76
63. Hair J, Hollingsworth CL, Randolph AB, Chong AYL (2017) An updated and expanded assessment of PLS-SEM in information systems research. Ind Manag Data Syst 117(3):442–458
64. Streukens S, Wetzels M, Daryanto A, De Ruyter K (2010) Analyzing factorial data using PLS: application in an online complaining context. In: Vinzi VE, Chin WW, Henseler J, Wang H (eds) Handbook of partial least squares. Springer, Berlin, pp 567–587
65. Kim J, Mohan K, Ramesh B (2014) Functional and nonfunctional quality in cloud-based collaborative writing: an empirical investigation. IEEE Trans Prof Commun 57(3):182–203
66. Yi MY, Davis FD (2003) Developing and validating an observational learning model of computer software training and skill acquisition. Inf Syst Res 14(2):146–169
67. Chin WW (1998) The partial least squares approach to structural equation modeling. In: Marcoulides GA (ed) Modern methods for business research. Lawrence Erlbaum Associates, Mahwah, pp 295–336
68. Kline TJ, Sulsky LM, Rever-Moriyama SD (2000) Common method variance and specification errors: a practical approach to detection. J Psychol 134(4):401–421
69. Chin WW, Gopal A (1995) Adoption intention in GSS: relative importance of beliefs. ACM SigMIS Database 26(2–3):42–64
70. Singh A, Malhotra M (2015) Security concerns at various levels of cloud computing paradigm: a review. Int J Comput Netw Appl 2(2):41–45
71. Baron RM, Kenny DA (1986) The moderator–mediator variable distinction in social psychological research: conceptual, strategic, and statistical considerations. J Pers Soc Psychol 51(6):1173–1182
72. Barlow JB, Warkentin M, Ormond D, Dennis AR (2013) Don't make excuses! discouraging neutralization to reduce IT policy violation. Comput Secur 39:145–159.
73. D'Arcy J, Devaraj S (2012) Employee misuse of information technology resources: testing a contemporary deterrence model. Decis Sci 43(6):1091–1124
74. Lee SM, Lee S-G, Yoo S (2004) An integrative model of computer abuse based on social control and general deterrence theories. Inf Manag 41(6):707–718
75. Li H, Zhang J, Sarathy R (2010) Understanding compliance with internet use policy from the perspective of rational choice theory. Decis Support Syst 48(4):635–645
76. Ifinedo P (2014) Information systems security policy compliance: an empirical study of the effects of socialisation, influence, and cognition. Inf Manag 51(1):69–79

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.