

Biometrics Technology Use and Its Relation to Information Security Policy Compliance: Nursing Staff Perspective

Mervat Abd Elmonem Noeman Aref¹, Hind Ismail Ali², Samah Elsayed Rashed³

¹Nursing Administration Department, Damanhur University, Egypt.

²Department of Nursing Sciences, College of Applied Medical Science, Prince Sattam bin Abdulaziz University, Wadi Addawasir, Kingdom of Saudi Arabia., ²Department of Nursing Administration, Sohag University, Egypt.

³Nursing Administration Department, Benha University, Egypt.

*Corresponding author: Mervat Abd Elmonem Noeman Aref, Email:Mervat.aref@nur.dmu.edu.eg

Abstract:

Background: Biometric identification technologies are rapidly expanding across healthcare sectors. These technologies offer secure methods for identifying nursing staff, thus enhancing confidentiality and compliance with information protection standards. The management of the hospital's information resources may be impacted by the nursing staff's perception of biometrics technology and information security. **Aims:** the present study aimed to assess biometrics technology use and its relation to information security policy compliance from nursing staff perspectives. **Research Design:** A descriptive correlational research design was utilized to conduct this study. **Study setting:** the study was conducted in critical care units at Benha University Hospital. **The study sample:** A Simple random sample of 339 nursing staff participants working in previous mentioned setting. **Data collection tools:** two tools were used; biometric technology use perception questionnaire, and information security policy (ISP) compliance questionnaire. **Results:** current study revealed that almost all of nursing staff had between a (43%) high level and (42%) moderate level of biometric technology usage perception and nearly half of them (45%) demonstrated a moderate level of information security policy compliance. **Conclusion:** there was a highly statistically significant positive correlation between nursing staff' biometric technology use perception and their ISP compliance. **Recommendation:** based on the study findings it is recommended to integrate the concepts of biometric technology and ISPs compliance into undergraduate and post graduate education, and the hospital administration should organize training programs, discussion groups, seminars, and workshops in the hospital and provide orientation about the importance, implementation and maintenance of biometric technology. Further study is needed to examine the elements that affect biometrics technology and information security policy, such as healthcare organizational culture, regulations, and technology developments.

Keywords: Biometrics technology, information security policy compliance, and Nursing staff.

1. Introduction

In the context of digital transformation and rapid technological advancement, the protection of intellectual properties rights and the enforcement of strong security of information have become essential for organizational operations (Stoumpos, et al., 2023). The combination of Internet of Things (IoT) and artificial intelligence (AI) within the healthcare sector has greatly enhanced efficiency, accuracy, and accessibility. IoT serves as a foundational technology for innovative smart healthcare systems, utilizing

sensors to gather data in real time for analysis. One of the important applications of IoT is biometric technology (Kraus, et al., 2021; Onesio-Ozigagunet al., 2024).

Biometric can be defined as measuring of a human being using physiological and behavioral features. The physiological characteristics allow for the identification and authentication of a person using a collection of identifiable and verifiable biometric information, including voice, fingerprint, iris, and facial data. (Banville, 2023). A person can be identified and described using these

biometric identifiers, which are unique, and quantifiable characteristics. Behavioral biometrics uses an individual's distinct interactions with technology and gadgets to find them. (Mason, et al., 2020).

According to **Habibu et al., (2022)** biometric technology' acceptance involve the measuring of three main areas: *first*; Perceived Ease of Use (PEOU): is the perception of feasibility and practicability of biometric system usage, *second*; Perceived Usefulness (PU): to what extent use of biometric is useful in operating tasks, mitigates heavy work load, and is more secure. The *third* is; Perceived Enjoyment (ENJ): the positive perception that biometric authentication reduces the problem of forgetting password problem and the familiarity with system.

Biometric security refers to the use of biometric data for authentication, access control, and identification. Biometric data is obtained by cameras and fingerprint readers, scanned, and then algorithmically assessed against data in a database (**Babu et al., 2024**). Biometric security has overcome the limits of previous computing days, and individuals all over the world now prefer to utilize biometric identification systems as an alternative to traditional password-based authentication techniques (**De Keyser, et al. 2021**). It eliminates the need to memorize passwords, is incredibly accurate in authenticating a person's identity, and works as a layer of protection against unwanted access, thereby meeting the current requirement for information security policy (ISP) (**Stylios, et al., 2022**).

A policy for information security is a framework of regulations that guide healthcare personnel in managing data and IT systems securely. It guarantees that only individuals with permission can access confidential information and encompasses topics such as access control, user authentication, remote access, and protection against malicious software. ISP compliance involves conforming to healthcare-specific regulations, standards, and laws concerning data security (**Amin et al., 2024**).

Compliance with ISP includes nine factors as follows; *information security knowledge sharing*: regularly exchange information security knowledge at work to reduce information risk, *information security collaboration*: believe that working with the information security team is necessary, *information security intervention*: information security training courses had impact on nurses' attitude towards security compliance, *information security experience*: information security practices are enhanced by security experiences, *attachment*: discuss the value of maintain organizational information secures with peers from nursing staff, *commitment*: nurse' dedication to protecting the organization's information resources, *personal norms*: it is not acceptable for nurse to disregard the organization's information rules, and security' regulations, *attitude towards compliance with ISOP*: adhering to ISOP is essential and advantageous, and *ISOP compliance behavioral intentions*: likely to follow ISOP in the future (**Safa et al., 2016; Ali et al., 2021 and Amin et al., 2024**)

In shared healthcare environments, biometric technologies usage with suitable ISP compliance offer a more secure method of patient identification, helping to prevent insurance fraud, reduce the costs associated with password management, and mitigate information security risks. They also facilitate the rapid identification of unconscious individuals and eliminate the need for passwords or PINs (**Afrizal et al., 2020**). Biometric recognition allows patients to register using fingerprints, thereby shortening waiting times during emergencies and checkups. This method is favored over traditional authentication systems due to its reliability, high security, and ability to prevent unauthorized access. Additionally, biometric systems reinforce hospital network security, protecting sensitive patient data from cyber attacks and fraudulent activity (**Dart & Ahmed 2023**).

1.1. Significance of the study

Nurses' perspectives on biometric technologies are pivotal to their effective implementation in healthcare settings. While

many nurses regard biometrics as secure, efficient, and privacy-protecting, concerns remain due to time constraints and resistance to technological change (La Corte, 2019; Wells, & Usman, 2024).). The intersection of biometrics and information security policy presents both potential and complexity. On one hand, biometric authentication helps mitigate issues like password sharing, unauthorized access, and identity theft; on the other, it raises concerns over privacy, technical errors, and staff reluctance due to unfamiliarity (Hamapa et al., 2024). Therefore, examining nurses' viewpoints offers valuable insight into the practical utility of biometric systems in promoting compliance with information security policies (Hathaliya et al., 2019). Few studies were done to examine study variables from nursing staff perspectives. Hence the current study aimed to assess biometrics technology use and its relation to ISP compliance from the perspectives of nursing staff.

1.2. Aim of the study:

This study aimed to assess biometrics technology use and its relation to ISP compliance from the perspective of nursing staff.

1.3. The Research Questions:

What is the relation between nursing staff's perception about biometric technology use and their ISP compliance?

2. Subjects and Methods

2.1. Research Design:

A descriptive correlational research design was utilized to conduct this study.

2.2. Setting:

The current study was conducted at Benha University Hospital, Benha, Egypt. It was conducted in Critical Care Units as follows: Coronary Care Unit (CCU), Intensive Care Unit (ICU), chest ICU, emergency, pediatric ICU, Hepatic ICU, and psychiatric ICU. The total

number of beds at these units is 118. The ICU units are the main units where the nurses use computer-based documentation and are linked with the informatics system of the laboratory and radiology departments.

2.3. Subjects

2.3.1. Subject Type

The study participants included a simple random sample of registered nurses recruited from Critical Care Units from the setting mentioned above

2.3.2. Subject Size

The sample size was calculated utilizing Slovin's Formula (Ryan, 2013):

$$\text{Sample Size} = N / (1 + N \cdot e^2), n = 741 / (1 + 741 * (0.04)^2) = 339.04 \approx 339$$

N = population size = 741 and e = margin of error = 0.04

So, Sample size = 339 nursing staff from previously mentioned settings and who have experience in the presently work department for at least six months.

2.4. Tools of Data Collection

Two tools were used to gather data for this study:

2.4.1: Biometric technology use perception questionnaire: It composed of two parts:

Part 1: Personal data form: It included data about age, marital status, gender, job, work unit, and years of experience.

Part 2: Biometric technology use perception questionnaire: A Structured questionnaire was adopted from Habibu et al., (2022) to examine the nursing staff's perception of the usage of biometric technology. This questionnaire consisted of 10 items arranged into three domains: Perceived Ease of Use (PEOU) (3 items), Perceived Usefulness (PU)

(4 items), and Perceived Enjoyment (ENJ) (3 items). A five-point Likert scale, ranging from (1) strongly disagree to (5) strongly agree, was used to rate the participants' responses.

2.4.2. Information security policy (ISP) compliance questionnaire: It was adopted from **Safa et al., (2016)** to describe nursing staff's information security compliance with the organization's policies. It consisted of 40 items divided into nine dimensions; information security knowledge sharing (6 items), information security collaboration (5 items), information security intervention (4 items), information security experience (4 items), attachment (4 items), commitment (4 items) personal norms (4 items), Attitude towards compliance with ISOP (4 items), and ISOP compliance behavioral intentions (5 items). A five-point Likert scale, ranging from (1) strongly disagree to (5) strongly agree, was used to rate the participants' responses.

The Scoring system of the data collection tools:

The upper limit of the alternatives for data collection tools was (5), and the lower limit of the alternatives was (1) = (4/5), so the length of the category is (0.8). It defines 5 descriptions, namely strongly agree (4.21 to 5.00), agree (3.41 to 4.20), neutral (2.61 to 3.40), disagree (1.81 to 2.60), and strongly disagree (1.00 to 1.80). Items scores estimated as follows: average items score < 2.5 for low level, from 2.5 to 3.5 for moderate level, and > 3.5 for high level.

Thus, the **level** of questionnaires total items was estimated as follows: < 50% for low level, 50% - 70% for moderate level, and > 70% for high level (**Sack, 2020**).

2.5. Methods

1.Preparatory phase; for data collection, the researchers viewed the national and international related literature using journals, textbooks, periodicals, and theoretical foundation understanding of the various aspects concerning the variables and topic of the study.

2.The study tools were translated into Arabic language and back translation for accuracy checking.

3.The tool's validity

The face and content of data collection tools were validated by a jury consisting of five nursing administration experts. The jury group members (Five professors of nursing administration at Benha, and Sohag University) judged the instruments for accuracy, thoroughness, and linguistic intelligibility (face validity). The significance of the items to be included in the tools was assessed by the jury group members (content validity). Minor changes, such modifying some sentences to fit the characteristics of various participants, were made in response to their recommendation.

4.Reliability of the tools

The internal consistency and homogeneity of the instruments were assessed using the Cronbach's Alpha test of reliability. Cronbach's alpha for Biometric technology use perception questionnaire was 0.83, which shows good level of internal consistency and Cronbach's alpha for ISP compliance questionnaire was 0.89 reflecting excellence internal consistency.

5.Administrative Design:

After outlining the goal and scope of the study, consent was sought from the responsible authorities (the Benha University hospital and Benha Faculty of Nursing) before the study could begin. In order to find an appropriate time to collect data from nursing staff, the researchers also met with the head nurse of each department.

6.Pilot study:

It was carried out on 33 nursing staff that included proportionately in the pilot study, representing 10 % of the total study subjects. It was conducted for ensuring tools clarity and feasibility. Also, to determine how long it will take to fill the tools. It ranged between 5-10 minutes for the Biometric technology using the perception questionnaire and ranged between 15-20 minutes for the ISP compliance

questionnaire. No adjustment was needed, and the pilot included within the study.

7. Ethical consideration:

Approval to conduct study was obtained, with approval code (103-m) from Ethical and Research Committee in the Faculty of Nursing, Official permission was issued from the Dean of the Faculty of Nursing to the Director of Benha University Hospital for obtaining their permission to conduct the study and solicit their assistance. The researchers met the head nurse of each department to determine a suitable time for data collection. The subjects involved in the study were informed of the purpose and nature of the study prior to its execution. Every subject was made aware that taking part in the study was entirely optional, and study participants gave their informed consent. The questionnaire sheets were coded to preserve the privacy of the collected data. Subjects were made aware of their freedom to withdraw from the study at any time and that the tools' content would only be utilized for research.

8. Fieldwork:

Data collection took about two months, from the beginning of April 2025 to the end of May 2025. The researcher met with the nursing staff and outlined the purpose and nature of the study as well as how to complete the questionnaires. This was done individually and through group meetings. The researcher distributed the questionnaire sheets to the participating nursing staff to fill them at work times, which were previously decided upon in consultation with each unit's head nurse based on the workload. Data was gathered four days a week while the researcher was present to clear up any confusion. The average number of sheets filled per day ranged between 10 and 12 sheets.

The randomization of nurses from the HR database followed a systematic and transparent process using a random number generator. First, obtain a complete and updated list of eligible nurses from the HR database, ensuring each nurse is assigned a unique identification number (employee ID). Once the full list is compiled, input the range of ID

numbers into a random number generator (through Microsoft Excel). Generate as many random numbers as needed based on the desired sample size. The nurses corresponding to those randomly selected numbers will form the study sample. This method eliminates selection bias and ensures each nurse has an equal chance of being included.

2. 6. Statistical Design

The Statistical Software Package for the Social Sciences (SPSS version 20) was utilized for statistical analysis. P-value ≤ 0.05 indicated significance, and when p-value ≤ 0.001 , a highly significant result was considered, while p-value > 0.05 indicated non-significance. The authors presented results in the form of frequency, percentage, mean, and standard deviation using descriptive statistics. Examine several aspects of the mean independent t-test results. For examining the relationship between variables Pearson correlation analysis was used. A scatter plot diagram shows the relationship between the two main variables and domains.

3. Results

Table 1 shows the personal characteristics of the study participants, where about half (48.38%) of participants were aged $30 \leq 40$. As regards gender and marital status, (74.04% & 64.60%) were females and married, respectively. Concerning years of work experience, nearly one third (44.25%) had $10 \leq 15$ years with ($X \pm SD = 11.61 \pm 5.52$). Besides that, more than half of the participants (73.16%) had a bachelor's degree in nursing.

Figure 1 and Table 2 present the study participants' perceptions of biometric technology usage, where almost all of them had between a (43%) high level and (42%) moderate level of biometric technology usage perception. Among the three measured domains of perception, Perceived Usefulness (PU) received the highest mean score (3.925 ± 1.162), followed by Perceived Ease of Use (PEOU) (3.249 ± 1.685). Overall, nursing staff participants exhibited a generally high perception of biometric technology, with a composite mean score of 3.579 ± 0.982 .

Figure 2 and Table 3 present the study participants' responses regarding ISP compliance, where depicted to present nearly half of the participants (45%) had a moderate level of compliance. ISOP compliance behavioral intentions were the first-ranked domain with 3.523 ± 0.077 , while information security experience came at the last with 2.561 ± 0.976 . Concerning that, the study participants had a moderate perception of ISOP compliance with 3.431 ± 0.127

Figure 3 and Table 4 demonstrate a statistically significant positive correlation between perceptions of biometric technology and ISP compliance ($r = .587$, $p < .001$). Additionally, strong positive correlations were observed among key perception domains. Notably, Perceived Ease of Use (PEOU) correlated strongly with collaboration ($r = .863$), information security experience ($r = .694$), and personal norms ($r = .837$). All statistically significant ($p < .001$). Perceived Usefulness (PU) also showed strong positive correlations with information security intervention ($r = .682$) and personal norms ($r = .729$).

Correlation data from Figure 3 further highlight strong relationships between biometric perceptions and compliance dimensions, particularly with information security intervention ($r = .801$), commitment ($r = .869$), and attitude toward compliance ($r = .663$). These findings suggest that positive perceptions of biometric systems significantly enhance secure behavioral intentions.

Additionally, PU is closely linked with commitment ($r = .752$), and perceived enjoyment (ENJ) shows a strong correlation with Attitude toward Compliance ($r = .871$) and Attachment ($r = .542$), indicating that engagement and perceived value play key roles in compliance.

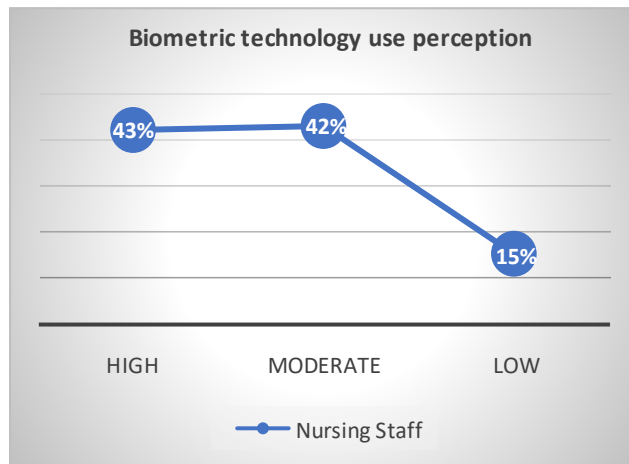
Overall, the scatter plot visually confirms that favorable perceptions of biometric technology are closely associated with stronger ISP compliance, underscoring the importance of designing usable and meaningful biometric systems in healthcare.

Table 5 reveals statistically significant differences in participants' perceptions of biometric technology based on demographic factors. Specifically, perception scores varied significantly by age ($p = .000$), with the highest mean among those aged 30–40 years; by years of experience ($p = .000$), with the highest mean (3.212 ± 0.885) among those with 10–15 years of experience; and by educational level ($p = .004$), with the highest mean (3.232 ± 0.886) observed in participants holding a master's degree.

Regarding ISP compliance, significant differences were also found by years of experience ($p = .000$) and age ($p = .000$), with the highest mean (3.782 ± 0.654) in both cases among participants aged 30–40 years and those with 10–15 years of experience.

Table (1): Frequency distribution of the study participants according to personal characteristics (N=339)

Items		No	%
Age X ±SD 31.5 ± 2.18	<30 yrs.	130	38.35
	30 ≤ 40yrs	164	48.38
	More than 40 years.	45	13.27
Gender	Male	88	25.96
	Female	251	74.04
Marital status	Married	219	64.60
	Unmarried	120	35.40
Years of experience X ± SD 11.61 ±5.52	1< 5 yrs.	51	15.04
	5 ≤ 10 yrs.	76	22.42
	10 ≤15 yrs.	150	44.25
	More than 15 years.	62	18.29
Educational level	Diploma	73	21.53
	Bachelor	248	73.16
	Master	18	5.31

**Figure (1) Nursing staff's perception levels regarding biometric technology use. (N=339)****Table (2): Mean score and standard deviation of nursing staff's perception regarding the use of biometric technology. (N=339)**

Variables	Average Mean	SD	Ranking
Perceived Ease of Use (PEOU)	3.249	1.685	2
Perceived Usefulness (PU)	3.925	1.162	1
Perceived Enjoyment (ENJ)	3.062	0.114	3
Total	3.579	0.982	

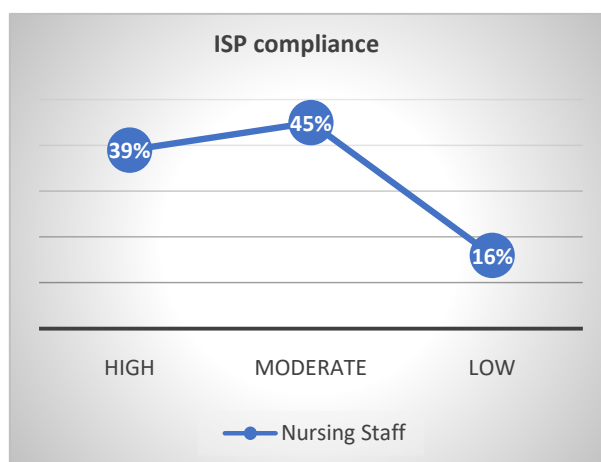


Figure (2): Nursing staff' levels regarding ISP compliance. (N=339)

Table (3): Mean and standard deviation of nursing staff' responses regarding ISP compliance. (N=339)

Variables	Average Mean	SD	Ranking
Information security knowledge sharing	3.107	0.685	5
Information security collaboration	3.051	1.134	8
Information security intervention	3.062	0.114	7
Information security experience	2.561	0.976	9
Attachment	3.142	0.871	3
Commitment	3.103	0.485	6
Personal norms	3.280	0.761	2
Attitude towards compliance with ISOP	3.121	0.881	4
ISOP compliance behavioral intentions	3.523	0.077	1
Total	3.431	0.127	

Figure (3) The scatter diagram showing the correlation coefficients between biometric technology use perception factors and various information security policy (ISP) compliance-related variables

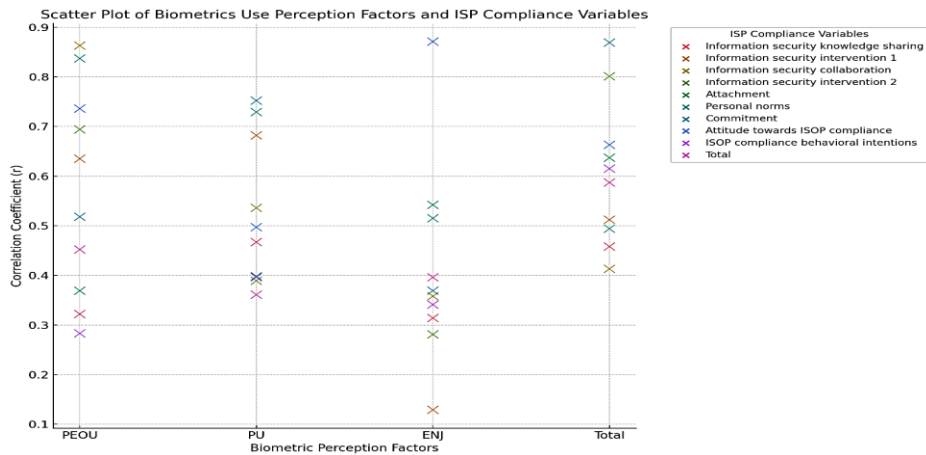


Table (4): Pearson Correlation between biometric technology use perception and ISP compliance. (N=339)

ISP compliance		Biometric technology uses perception.			
		Perceived Ease of Use	Perceived Usefulness	Perceived Enjoyment	Total
Information security knowledge sharing	r	.322	.467	.314	.458
	P	.000	.014	.219	.000
Information security collaboration	r	.863	.536	.358	.413
	P	.000	.027	.069	.010
Information security intervention	r	.635	.682	.129	.512
	P	.000	.001	.009	.002
Information security experience	r	.694	.389	.281	.801
	P	.000	.049	.011	.052
Attachment	r	.369	.398	.542	.637
	P	.558	.008	.008	.051
Commitment	r	.518	.752	.369	.869
	P	.010	.017	.000	.000
Personal norms	r	.837	.729	.515	.494
	P	.000	.001	.051	.000
Attitude towards compliance with ISOP	r	.736	.497	.871	.663
	P	.041	.019	.006	.003
ISOP compliance behavioral intentions	r	.283	.396	.341	.615
	P	.001	.053	.113	.000
Total	r	.452	.361	.396	.587
	P	.002	.005	.000	.000

Table (5): Relationship between total study variables and study participants' characteristics (N=339)

Study participants' characteristics	ISP compliance		Biometric technology uses perception	
	M(SD)	t/F (P)	M(SD)	t/F (P)
Age				
<30 yrs.	2.632±.411	7.23 .341	2.692±.778	11.47 .000**
30 ≤ 40yrs	3.017±.591		3.782±.654	
More than 40 years.	2.424±.544		2.162±.897	
Gender				
Male	2.741±.533	1.650 .040*	2.889±.736	1.841
Female	2.874±.714		3.077±.892	.051
Marital status				
Unmarried	2.794±.686	3.472 .075	3.042±.883	.053
Married	3.070±.633		3.036±.796	.958
Years of experience				
1< 5 yrs.	2.869±.645	9.508 .050*	2.701±.469	11.303 .000**
5 ≤ 10 yrs.	2.847±.714		2.825±.816	
10 ≤15 yrs.	3.212±.885		3.254±.886	
More than 15 years.	3.192±.516		3.116±.886	
Educational level				
Diploma	2.863±.7083	.737 .461	3.77±.6244	.383
Bachelor	2.893±.539		2.262±.597	.004*
Master	3.232±.886		3.012±.758	

* Statistically significant difference $P \leq 0.05$ ** Highly statistically significant difference $P \leq 0.00$

4-Discussion

This study aim was to assess biometric technology use and its relation to ISP compliance from the perspectives of nursing staff. The study findings revealed that favorable perceptions of biometric technology are closely associated with stronger ISP compliance, highlighting the importance of designing usable and meaningful biometric systems in healthcare.

Biometric technology use perception

Our findings showed that study participants had a high perception regarding the use of biometric technology. Among its domains, PU was ranked first, followed by PEOU. This can be interpreted that many factors can contribute in study participants' understanding of the importance, applications, and benefits of biometrics in healthcare as follows; The majority of study participants are bachelor degree, the minority hold master degree and more than one third of them are considered newly graduated with age less than 30 years and contemporary the incorporating

biometrics topics into nursing curricula. Also, study participants are intensive care nurses who deal with technologies and advanced systems and devices in ICUs and deal with a computer-based documentation system with biometric security. Moreover, the attendance signature is now a fingerprint biometric signature in their workplace.

Besides, now many of the nursing staff were owning or dealing with digital technologies devices with biometric security, such as fingerprint smart phones, computers, Keyboards, microphones, digital cameras, iris cameras, and fingerprint scanners. They use biometrics instead of writing memorized passwords and find it easier and solve forgetting password problems. Our results could be supported by **Hamapa et al., (2024)** as they found that the majority of the study's participants have good awareness about the advantages and disadvantages of biometric technologies. Thus, the majority of them have no objection, and they are in favor of biometric technology implementation.

Also, **Anne et al., (2020) and Stylios et al., (2022)** reported that the study participants have trust in the biometrics system, and in the future, they agreed to face changes in the current system, as well as they were already aware of biometrics, and they will readily accept the biometric system's installation and adoption in daily life and the workplace. Similar to our findings, **Mwapasa et al., (2020) and Cambaco et al., (2021)** reported that healthcare professionals generally accept the biometric prototype registration system that has been piloted. The potential advantages of the tested biometric prototype registration over the real registration system / paper-based registration, which are thought to be ineffective and problematic, are linked to its acceptability. (**Huang, 2023**).

Conversely, in **Garg et al., (2021)** study participants highlighted that despite biometric many privileges and benefits, its devices can be potential sources of infection transmission due to contamination from different users' repeated contact or touch. Also, **Mecke et al., (2024)** mentioned that most participants were able to name examples and stated that they use biometrics in their daily lives, but they were still having trouble elucidating the underlying ideas. They provided insight into participants' misunderstandings, coping mechanisms for authentication errors and possible breaches, and opinions regarding the overall usability and safety of biometrics.

Information security policy compliance

Our findings showed that the study participants had a moderate perception of ISOP compliance. Among its domains, the ISOP compliance behavioral intentions were the first-ranked one. It can be interpreted as the study setting is one of Egyptian hospitals which a taking valuable steps to comply with General Authority for Healthcare Accreditation and Regulation (GAHAR) standards and has clear accountability measures and routine monitoring that reinforce the importance of compliance with information security, and a culture that emphasizes security, along with strong leadership support and clear communication, fosters compliance intention and behavior. Also, study participants deal with a computer-based

documentation system and know the importance of secure data from being breached.

In the same respect, **McCarthy et al., (2019)** highlighted that nurses who deal with electronic documentation are more concerned with data confidentiality. Additionally our findings goes with **Alrasheeday et al., (2023)** and **Yas et al., (2024)** who reported that staff nurses especially younger nurses appeared to get more motivation and enthusiasm at work and feel more responsibility for patients' safety and consider it as main part of their job and according to **Abd Elhamid et al., (2020)** critical care nurses are prone for compliance with environmental and work safety and data security protocols and guidelines. Similar to our findings, studies have demonstrated high perception and intention of nurses for ISOP compliance, as in **Li et al., (2021)** who reported that the participants generally indicated a higher level of tendency toward policy compliance. Also, **Bakkar et al., (2018)** findings emphasized the concept that sensitive patient data should always be safeguarded to defend their right to privacy is supported by nurses' emphasis on the confidentiality aspect of information security.

Our findings also, showed that among information security policy compliance domains, the information security experience was the last ranked one. The lower level of nursing staff' information security experiences can be interpreted as heavy workload and time pressures in critical care units can limit nurses' opportunities to engage with security-related tasks, limited access to up-to-date security tools or resources hampers security' practical experience development, limited exposure to security practices or security procedures in their daily routines. In this context **Yeng et al., (2022)** emphasis that nurses ' load and work-related factors can influence their experience with ISOP compliance. This perspective could be supported by **Alshare et al., (2018)** as they found that participants had high perception levels and complied with ISP compliance, and their practical experience was still limited.

The correlation between Biometric technology use and information security policy compliance

The study findings represent a statistically significant positive correlation between nursing staff biometric technology use perception and their ISP compliance. This study emphasizes biometric identification technologies' potential to increase healthcare effectiveness and data security, and integrity. This result can be interpreted as nurses' biometric technology awareness and use strengthening nursing staff's positive perception of security importance and facilitating policy compliance, enabling them to implement appropriate policies to safeguard patient data. Also, they became more knowledgeable that improper management or neglect of security policy considerations in biometric can undermine security and confidentiality of patient data and make it more prone to cyber breach threats.

Similar to our findings, studies have demonstrated the role of biometric technology and electronic information system in enhancing security compliance' intention and intervention; **Habibu et al., (2022)** pointed out that the use of biometric technology is essential for enhancing the security of various systems that need user verification and the advancement of information technologies. Its implementation guarantees effective identification of individual and biometric identifiers are not as easily forgotten or lost as passwords. Also, **Hadzidedic et al., (2022)** found that fingerprint-based identification was seen to be a practical and safe technique and considered an effective system to protect data. In the same respect, the study of **Hamapa et al., (2024)** emphasizes the potential for biometric identification technologies to enhance the efficiency, security, and integrity of healthcare data. Additionally, **Afrizal et al., (2020)** reported that perceived ease-of-use and perceived security had a positive effect and correlated with the use of e-filing and security compliance intention. Moreover, **Mason et al., (2020)** emphasized the important role of biometric awareness in enhancing nurses' positive perception toward security policy compliance. In the same line, **Kang & Seomun,**

(2021) highlights that when handling patient data, nurses should understand the significance of information security., especially electronic data, and that related education is essential.

Besides that, study findings implied that there were many strong positive correlations among the variables' domains. Mainly, perceived ease of use had a statistically significant, strong positive correlation with information security intervention, information security collaboration, and personal norms. Also, the domain perceived usefulness had a statistically significant, strong positive correlation with information security intervention and personal norms. This implies that the integration of biometric authentication may influence nursing staff's behavior, encouraging their more diligent adherence to security policies due to the perceived robustness of biometric verification. They showed that biometrics, when applied in healthcare, will be easy to use, decrease workload, and improve efficiency. As a result, they will apply and comply with its information security intervention and standards for maintaining its applications and sustainability. From these perspectives, **Stylios et al., (2022)** pointed out that perceived usefulness is the primary driver of behavioral intention to embrace the technology. Also, their results showed that individuals who are less interested and consider the ease of use of the technology are not willing for achievement of greater security compliance.

In the same respect, the **Kraushaar et al., (2025)** study provides new insights into how a high standard of information security compliance among nurses could be achieved through strengthening security work awareness and engagement . And usefulness perception had a significant positive effect on information security-related compliance. Also, this result is consistent with **Mosqueda, (2023).** who reported that the perceived importance of ISPC was positively correlated with the use of technologies and measures that minimize breaches. Similar to our results, the results of **Dart & Ahmed, (2023).** Which showed that the perceived technology' usefulness and security controls considered the most significant factor that can influence staff beliefs and behaviors. In the same line the study of

LaCorte, (2019). Highlighted the role of nurses' personal norms, including values and beliefs, in adopting biometric technologies. Conversely, **Kang & Seomun, (2021)** mentioned that there was a discrepancy between intention and actual behavior of ISOP compliance.

The difference between staff nurses in their biometric technology use and ISP compliance

Our study findings demonstrated a statistical significance difference between staff nurses about their biometric technology use and ISP compliance according to their age, work experiences and educational level, demonstrating that staff nurses with higher education level especially master degree have high perception to biometric technology use and are more prone for ISOP compliance, this reflect that they take chance to with contemporary nursing curricula that became more emphasized on biometric technology and AI applications in health care, including its topics as patient safety and ethical considerations in managing patient electronic information. Also, our results shed light on the role of work experience in the perception of biometric technology use and security compliance, demonstrating that staff nurses with high work experience have a positive perception of biometric technology use and a high intention to comply with security standards. This reflects what was mentioned before, as nurses who work more with technology perceived it as easy to use and more important for work efficiency, and knowing the importance of securing patient data from cyber security breaches. In the same respect, **Al-Jafar et al., (2021)** showed professionals with greater work experience were more likely to follow sound cyber security procedures. Moreover, **Ali et al., (2021)** study revealed that the experience and prior information and security training and education were statistically significant regarding ISP compliance, and security policy information competence was positively associated with information security attitudes. Similar to our results, the results of **Dart & Ahmed, (2023)** and **Keshav, & Gupta, (2023)** showed that the perceived value of security measures relies on education and training proved out to be the most important

element affecting the attitudes and actions of the nursing staff.

5- Conclusion:

The findings of the current study revealed that nearly half of the critical care units' nursing staff demonstrated a high level of perception toward the use of biometric technology, while approximately half showed a moderate level of compliance with information security policies. A highly statistically significant positive correlation was identified between nurses' perceptions of biometric technology use and their compliance with information security policies. Additionally, significant differences were observed between participants' perceptions of biometric technology and their personal and professional characteristics. These results highlight the importance of promoting awareness and understanding of biometric technologies to enhance policy compliance among nursing staff.

6-Recommendations

Based on study findings it is recommended to:

- Integrate the concepts of biometric technology and ISPs compliance into undergraduate and post graduate nursing' education.
- Organize training programs, discussion groups, seminars, and workshops for nursing staff at their workplace to spread awareness of the importance of this technology, using it and ISPs
- The hospital administration should concentrate more on developing and utilizing a biometric network system to prevent unwanted unsafely events in various aspects and to offer security.
- Additionally, the necessary policies and legislation to preserve the data of staff and the entire hospital community if biometrics are used need to be developed.
- Further study is needed to examine the elements that affect biometrics technology

and information security policy, such as healthcare organizational culture, regulations, and technology developments.

References:

- Abd Elhamid, E. A., Abdallah, N. E. E., & Abd Elrahman, S. M. (2020). Nurses' compliance with patient and environmental safety guidelines in critical care units. 9 (2): 61-67
- Afrizal Tahar, Hosam Alden Riyadh , Hafiez Sofyani , Wahyu Eko Purnomo. (2020). Perceived Ease of Use, Perceived Usefulness, Perceived Security, and Intention to Use E-Filing: The Role of Technology Readiness. Journal of Asian Finance, Economics and Business Vol 7 No 9 537–547.
- Ali, R. F., Dominic, P. D. D., Ali, S. E. A., Rehman, M., & Sohail, A. (2021). Information security behavior and information security policy compliance: a systematic literature review for identifying the transformation process from noncompliance to compliance. Applied Sciences;11(8): 3383. DOI:10.3390/app11083383.
- Al-Jafar E, Abdulsalam Y, AlDuaij S.(2021). Information Security Awareness and Behaviors of Health Care Professionals at Public Health Care Facilities. 12(04): 924-932 DOI: 10.1055/s-0041-1735527
- Alrasheeday, A. M., Alshammari, B., Alkubati, S. A., Pasay-An, E., Albloushi, M., & Alshammari, A. M. (2023, August). Nurses' attitudes and factors affecting the use of electronic health records in Saudi Arabia. In *Healthcare* (Vol. 11, No. 17, p. 2393). MDPI.
- Alshare K, Lane P, Lane M.(2018). ISP compliance: a higher education case study. Information & Computer Security. 26(3):91-108. DOI:10.1108/ICS-09-2016-0073
- Amin, M. A., Tummala, H., Shah, R., & Ray, I. (2024). Balancing Patient Privacy and Health Data Security: The Role of Compliance in Protected Health Information (PHI) Sharing. *arXiv preprint arXiv:2407.02766*.
- Anne, N., Dunbar, M. D., Abuna, F., Simpson, P., Macharia, P., Betz, B., Cherutich, P., Bukusi, D., & Carey, F. (2020). Feasibility and acceptability of an iris biometric system for unique patient identification in routine HIV services in Kenya. *International Journal of Medical Informatics*, 133, 104006. <https://doi.org/10.1016/j.ijmedinf.2019.104006>
- Babu, A., Raoul, E., Kassahun, G., Dufour, I., Mandal, D., & Thuau, D. (2024). Programmable Polymeric-Interface for Voiceprint Biometrics. *Advanced Materials Technologies*, 9(4), 2301551.
- Bakkar M, Khelalfa H, Mckay E.(2018). Perception of information systems security: serving the healthcare industry in Dubai. International Journal of Internet and Enterprise Management. 9(1). 58-89. DOI: 10.1504/IJEM.2018.098935.
- Banville, M. C. (2023). Am I who I say I am? the illusion of choice: biometric identification in healthcare. East Carolina University.
- Cambaco O, Gachuhi N, Distler R, Cuinhane C, Parker E, Mucavele E, (2021). Acceptability and perceived facilitators and barriers to the usability of biometric registration among infants and children in Manhica district, Mozambique: A qualitative study. PLoS ONE. 16(12). DOI:10.1371/Journal.Pone.0260631
- Dart M, Ahmed M. (2023). Evaluating Staff Attitudes, Intentions, and Behaviors Related to Cyber Security in Large Australian Health Care Environments: Mixed Methods Study JMIR Hum Factors;10:e48220. DOI: 10.2196/48220.
- De Keyser, A., Bart, Y., Gu, X., Liu, S. Q., Robinson, S. G., & Kannan, P. K. (2021): Opportunities and challenges of using biometrics for business: Developing a research agenda. Journal of Business Research, 136, 52-62.
- Garg, S., Achra, A., Tiwary, N. K., Nirmal, K., Arora, S. K., Shulania, A., & Duggal, N. (2021). Change in perception regarding the use of Biometric devices at a tertiary care hospital given COVID-19. Journal of Patient Safety and Infection Control, 9(1), 17-21. DOI:10.4103/jpsic.jpsic_3_21.
- Habibu T, Luhanga E, Sam A.(2022). Assessment of how users perceive the usage of biometric technology applications. Recent Advances in Biometrics. 45. Intech Open. <https://www.intechopen.com/chapters/80525> DOI:10.5772/intechopen.101969
- Hadzidedic, S., Fajardo-Flores, S., & Ramic-Brkic, B.(2022). User perceptions and use of authentication methods: insights from youth in Mexico and Bosnia and Herzegovina. Information & Computer Security. DOI: 10.1108/ICS-07-2021-0105.
- Hamapa A, Zulu J, Khondowe O, Hangulu I.(2024). Healthcare workers' perceptions and user experiences of biometric technology in the selected healthcare facilities in Zambia. Discover Public Health. 21(47).<https://link.springer.com/article/10.1186/s12982-024-00167-0> DOI.ORG/10.1186/S12982-024-00167-0
- Hathaliya, J. J., Tanwar, S., Tyagi, S., & Kumar, N. (2019). Securing electronic healthcare records in healthcare 4.0: A biometric-based approach. *Computers & Electrical Engineering*, 76, 398-410.

- Huang H, Lin J. (2023).** Inconsistencies Between Information Security Policy Compliance and Shadow IT Usage. *Journal of Computer Information Systems*. 64(4), 554–564. DOI:10.1080/08874417.2023.2234318
- Kang J, Seomun G. (2021).** Information security in nursing: a concept analysis. *ANS. Advances in Nursing Science*. 44(1): 16–30. DOI:10.1097/ANS.0000000000000330
- Keshav, R., & Gupta, S. (2023).** Compliance challenges in the healthcare sector: A review of legal and regulatory frameworks. *Health Law Review*, 41(1), 52-63.
- Kraus, S., Schiavone, F., Pluzhnikova, A., & Invernizzi, A. C. (2021).** Digital transformation in healthcare: Analyzing the current state-of-research. *Journal of business research*, 123, 557-567.
- Kraushaar J, Bohnet-Joschko S. (2025).** The Role of the Organization in Promoting Information Security-Related Behavior among Residents in Hospitals in Germany: Cross-Sectional Questionnaire Study. *J Med Internet Res*. 7;27:e46257. doi: 10.2196/46257.
- LaCorte, M. (2019).** Factors Influencing Nurses' Acceptance of Biometric Information Technology in Hospitals: A Correlational Study (Doctoral dissertation, Capella University).
- Li L, Shen Y, Han M. (2021).** Perceptions of Information Systems Security Compliance: An Empirical Study in Higher Education Setting. DOI:10.24251/HICSS.
- Mason, J., Dave, R., Chatterjee, P., Graham-Allen, I., Esterline, A., & Roy, K. (2020).** An investigation of biometric authentication in the healthcare environment. *Array*, 8, 100042.
- McCarthy, B., Fitzgerald, S., O'Shea, M., Condon, C., Hartnett Collins, G., Clancy, M., & Savage, E. (2019).** Electronic nursing documentation interventions to promote or improve patient safety and quality care: A systematic review. *Journal of nursing management*, 27(3), 491-501.
- Mecke L, Saad A, Prange S, Gruenefeld U, Schneegass S and Alt F. (2024).** "Do They Understand What They Are Using? - Assessing Perception and Usage of Biometrics." P:3-12. DOI:10.48550/Arxiv.2410.12661
- Mosqueda J. (2023).** Perceptions and Knowledge of Information Security Policy Compliance in Organizational Personnel. Doctoral dissertation, Walden University Scholar Works. 116-117.
- Mwapasa, M., Gooding, K., Kumwenda, M., Nliwasa, M., Kaswaswa, K., Sambakunsi, R., & Desmond, N. (2020).** "Are we getting the biometric bioethics right?"—The use of biometrics within the healthcare system in Malawi. *Global Bioethics*, 31(1), 67-80.
- Onesi-Ozigagun, O., Ololade, Y. J., Eyo-Udo, N. L., & Oluwaseun, D. (2024).** AI-driven biometrics for secure fintech: Pioneering safety and trust. *Journal Name Unspecified*.
- Ryan, T. P. (2013).** Sample size determination and power. Wiley. <https://doi.org/10.1002/9781118439241>
- Sack, H. (2020).** Rensis Likert and the Likert scale method. SciHi Blog. Retrieved from <https://scihi.org/rensis-likert/>
- Safa N, Solms R, Furnell S (2016).** Information security policy compliance model in organizations. *Computers & security* 56 (2016) 1–13
- Stoumpos, A. I., Kitsios, F., & Talias, M. A. (2023).** Digital transformation in healthcare: technology acceptance and its applications. *International journal of environmental research and public health*, 20(4), 3407.
- Stylios I, Kokolakis S, Thanou O, Chatzis, S. (2022).** Key factors driving the adoption of behavioral biometrics and continuous authentication technology: an empirical research. *Information & Computer Security*. 30(4). DOI:10.1108/ICS-08-2021-0124
- Wells, A., & Usman, A. B. (2024).** Privacy and biometrics for smart healthcare systems: attacks and techniques. *Information Security Journal: A Global Perspective*, 33(3), 307-331.
- Yas, N., Elyat, M. N. I., Saeed, M., Shwede, F., & Lootah, S. (2024).** The Impact of Intellectual Property Rights and the Work Environment on Information Security in the United Arab Emirates. *Kurd. Stud*, 12(1), 3931-3948.
- Yeng, P. K., Fauzi, M. A., & Yang, B. (2022).** A comprehensive assessment of human factors in cybersecurity compliance toward enhancing the security practice of healthcare staff in paperless hospitals. *Information*, 13(7), 335.