Multidisciplinary Reviews

QUESTIONNAIRES APPLICATION
Published Online: February 5, 2025
https://doi.org/10.31893/multirev.2025195

Evaluating password security compliance in a Phuket private hospital: A UTAUT-based analysis

Pita Jarupunphol[a] | **Siwatchaya Suksai**[b] | **Wipawan Buathong**[a]

[a]Digital Technology Program, Phuket Rajabhat University, Thailand.
[b]Health Benefits, Bangkok Hospital Phuket, Thailand.

Abstract The study presented focuses on evaluating password security compliance within a private hospital in Phuket, employing the Unified Theory of Acceptance and Use of Technology (UTAUT) framework. Descriptive statistics reveal that 416 healthcare professionals participated in the survey, with 55% female. Age analysis showed that nearly half (48.6%) of participants were under 30, and 85.3% held a bachelor's degree. Most respondents adhered to recommended password security practices, including using passwords with 8-10 characters and incorporating numbers, uppercase letters, and special characters. However, a significant vulnerability was observed as 83.41% of respondents used the same password across multiple accounts. Statistical analysis using Structural Equation Modeling (SEM) indicated that performance expectancy (PE), effort expectancy (EE), and social influence (SI) significantly influenced behavioral intention (BI) to comply with password security practices. PE had the highest impact ($\beta = 0.56$, $p < 0.001$), followed by EE ($\beta = 0.26$, $p < 0.001$), and SI ($\beta = 0.21$, $p = 0.002$). Facilitating conditions (FC) significantly affected actual usage (USE) with a moderate impact ($\beta = 0.12$, $p = 0.036$). Age and experience moderated the relationships between these constructs, suggesting that younger and less experienced employees were more influenced by ease of use and performance expectations, while older staff relied more on facilitating conditions. This study contributes to the understanding of how various factors influence password security compliance in healthcare, emphasizing the need for tailored interventions based on demographic differences to enhance security practices effectively.

Keywords: behavioral intention, cybersecurity, password security, structural equation modeling, UTAUT

1. Introduction

Passwords, the most commonly used form of authentication, are crucial in securing access to computers, accounts, and databases, acting as a critical mechanism to protect personal, financial, and confidential data from unauthorized access (Nanda et al., 2024). The NIST (National Institute of Standards and Technology 2017) and ISO/IEC 27001:2022 have established comprehensive guidelines for password security, emphasizing the importance of password strength in preventing unauthorized access and ensuring data integrity and security. Currently, password security is a critical component of security within healthcare organizations, serving as the primary defense against unauthorized access to electronic health records, patient data, and other vital systems. The criticality of password security in healthcare is underscored by the sensitivity of patient medical records and financial data (Dickerson, 2022). It is also about patient safety and trust, making it a crucial aspect of healthcare operations (Javaid et al., 2023; Kuo et al., 2021). As such, password security practices within healthcare institutions must be robust and adaptive to counter the evolving landscape of cyber threats (Inglesant & Sasse, 2010; Sullivan et al., 2023).

A significant component of such practices involves ensuring that all personnel know and comply with password security practices (Humaidi & Balakrishnan, 2017). This often includes using complex passwords that combine letters, numbers, and symbols and changing passwords regularly to reduce the risk of unauthorized access (Ezugwu et al., 2023). Research highlights that the strength of a password can significantly deter potential cyberattacks. Studies indicate that longer passwords contain various character types and are less susceptible to brute-force attacks (Zimmermann et al., 2022). Moreover, password management policies that enforce regular updates and prevent the reuse of old passwords effectively enhance security (Kuo et al., 2021). Despite these advancements, implementing robust password security practices in healthcare remains challenging due to various factors, including resistance to change, the complexity of healthcare systems, and the need for rapid access to patient information in emergencies (O’Brien et al., 2020).

Moreover, it is crucial to consider various factors that influence user acceptance of security policies (Demsash et al., 2024). Research indicates that users’ perceptions of password creation and management significantly influence their acceptance and usage. For example, misunderstandings of the purpose and functionality of password creation can deter users from adopting these practices despite their potential benefits in enhancing security (Fagan et al., 2017). Users with higher

Received: October 18, 2024 | Accepted: December 6, 2024

computer proficiency find password managers convenient and secure, suggesting that user experience and familiarity with technology are critical factors in accepting such tools (Jamil et al., 2021).

The implementation of comprehensive cybersecurity frameworks, such as the essentials of cybersecurity in healthcare organizations (ECHO) framework, can guide healthcare institutions in complying with password security practices (O'Brien et al., 2020). These frameworks advocate incorporating user-friendly tools that enhance compliance with security policies while minimizing the burden on healthcare professionals. However, the effectiveness of password security compliance in healthcare settings is contingent upon user acceptance and is influenced by several factors (Kuo et al., 2021). Moderation analysis in cybersecurity studies is crucial for understanding the differential effects of predictors on diverse demographic groups, especially given the nature of healthcare professionals' interactions with password security practices.

1.1. UTAUT framework

UTAUT is a comprehensive framework that explains user intentions to utilize information systems and subsequent usage behavior. UTAUT integrates elements from various technology acceptance models, including the technology acceptance model (TAM) and activity theory, to provide a robust theoretical foundation for understanding technology adoption (Davis, 1993; Demsash et al., 2024). The UTAUT framework (Venkatesh et al., 2003) has been widely applied to explain user intentions to adopt various technologies, especially in highly regulated industries such as healthcare (Demsash et al., 2024). The UTAUT framework is built around four principal constructs that influence the behavioral intention (BI) to use technology (Venkatesh et al., 2003; Williams et al., 2015):

1. Performance expectancy (PE): This construct reflects the degree to which an individual believes that using a particular technology will enhance job performance. PE significantly predicts the BI of various information and communication technologies (ICTs), including mobile health applications (Demsash et al., 2024; Diel et al., 2023).
2. Effort Expectancy (EE): EE gauges the perceived ease of use associated with a technology. EE can lead to increased BI of new ICT applications, particularly in healthcare settings where usability is crucial (Demsash et al., 2024).
3. Social Influence (SI): SI pertains to how individuals perceive that essential others (e.g., peers, superiors) believe that they should use a new technology. Social influence encompasses the perceived norms and expectations established by reference groups, which can drive compliance and identification among healthcare professionals (Diel et al., 2023; Govindarajan et al., 2023). In healthcare, this construct emphasizes the role of the social context in shaping password security compliance (Williams et al., 2015).
4. Facilitating Conditions (FC): FC refers to the resources and support available to individuals to use technology effectively. FCs include supportive resources for healthcare staff to comply with password security practices (USE) (Diel et al., 2023).

The UTAUT posits that PE, EE, and SI significantly influence users' behavioral intentions (BIs) to adopt new technologies (Venkatesh et al., 2003). The relationships between these constructs and BI can be represented mathematically below, where ϵ represents the unexplained variance in behavioral intention, and β1, β2, and β3 are the coefficients representing the impacts of performance expectancy (PE), effort expectancy (EE), social influence (SI), and facilitating conditions (FC), represented in equation (1).

$$BI = \beta_0 + \beta_1 PE + \beta_2 EE + \beta_3 SI + \epsilon \quad (1)$$

BI represents the user's intention to engage with a technology. It is a critical predictor of actual usage behavior (USE). The relationship between BI and USE is well-documented in the literature, with studies showing that higher intentions correlate with increased usage (AlQudah et al., 2021a; Ketikidis et al., 2012). In addition to BI, FC is another primary condition influencing USE. In healthcare, the successful implementation of technologies will depend on users' intentions and the availability of resources and support systems that facilitate their password security compliance (Ketikidis et al., 2012). For example, facilitating conditions, defined as the belief that an adequate organizational or technical infrastructure exists to support new systems, are crucial for technology adoption (Diel et al., 2023). This complexity necessitates tailored implementation strategies that consider these contextual needs to ensure the effective uptake and utilization of health technologies (Breneol et al., 2022). The relationships among the BI, FC, and actual use (USE) can be expressed as equation (2).

$$USE = \gamma_0 + \gamma_1 BI + \gamma_2 FC + \epsilon \qquad (2)$$

1.2. UTAUT applications

The UTAUT model has demonstrated high predictive power, explaining approximately 70% of the variance in users' intentions to adopt information systems (Diel et al., 2023). For example, the model has been effectively applied in healthcare contexts to assess health professionals' acceptance of mobile-based clinical guidelines, revealing critical insights into factors that promote technology use in practice (Demsash et al., 2024). Understanding and applying the UTAUT framework remains essential for fostering effective technology adoption and ensuring improved health outcomes. In the context of password security compliance, these constructs can be adapted to examine factors that affect healthcare professionals' adherence to password security practices. With respect to password security compliance, the PI relates to the perceived benefits of complying with password security practices. Healthcare professionals may recognize that robust passwords are critical for safeguarding sensitive patient information and preventing unauthorized access, thereby protecting their organization and professional integrity (Barchielli et al., 2021). EE assesses the ease of password security compliance. Password managers can significantly reduce the cognitive load associated with remembering multiple complex passwords, thus increasing compliance (Breneol et al., 2022). As healthcare staff become accustomed to utilizing these tools, they may find it easier to follow security practices without compromising the quality of patient care. In addition, SI encompasses the impact of colleagues and organizational culture on individual behavior. In healthcare settings, peer pressure and leadership initiatives can promote a culture of security awareness, encouraging staff to adhere to robust password security practices (Ayatollahi & Shagerdi, 2017). Regular training and awareness programs can enhance this influence, improving compliance rates.

FC involves the resources and support available to facilitate the desired behavior. In password security compliance, healthcare organizations must provide training, tools, and resources to ensure that staff can implement robust password practices effectively (Ezugwu et al., 2023). Regular audits of password practices and user access reviews also contribute to a supportive environment for compliance (Ayatollahi & Shagerdi, 2017; Ezugwu et al., 2023). Integrating password management tools into the UTAUT framework primarily highlights their role in enhancing password security compliance in healthcare settings. These tools simplify the generation and storage of strong passwords and provide features such as encryption and cross-device accessibility, making it easier for healthcare professionals to adhere to security protocols without sacrificing efficiency (Uwizeyemungu et al., 2019). By aligning these tools with UTAUT constructs, organizations can understand how to encourage compliance and foster a secure working environment. Moreover, the cognitive aspects of password creation and management have been explored in the literature, revealing that users' cognitive styles and visual behaviors can affect password strength (Bimerew and Chipps, 2022; Katsini et al., 2019).

In addition to cognitive factors, the cultural context plays a significant role in acceptance of technology. How healthcare professionals' attitudes toward technology can be influenced by cultural values, which may affect their acceptance of password management tools, is discussed (Metallo et al., 2022). As such, integrating password strength creation into existing healthcare systems must consider the barriers to technology acceptance identified in previous studies. For example, Alqudah et al. (2021a) conducted a systematic review highlighting the factors influencing technology acceptance in healthcare, including usability, perceived benefits, and the overall impact on patient care. Addressing these barriers is essential for fostering a conducive environment for adopting password management solutions. The effectiveness of password strength compliance in healthcare settings can be evaluated through the lens of the UTAUT, which integrates cognitive, cultural, and contextual factors into the analysis. According to the UTAUT model, gender, age, and experience can impact various constructs. For example, gender affects PE, EE, and SI; age influences PE, EE, SI, and FC; and experience impacts EE, SI, and FC. In this case, the research objectives for this study can be outlined as follows:

1. To investigate the behavioral factors influencing healthcare professionals' adherence to password security practices within private healthcare via the UTAUT framework.
2. To assess the impact of key predictors such as performance expectancy (PE), effort expectancy (EE), social influence (SI), and facilitating conditions (FC) on healthcare professionals' behavioral intention (BI) and actual compliance with password security practices.
3. To explore the moderating effects of demographic variables, specifically age and experience, on the relationships between the UTAUT constructs (PE, EE, SI, and FC) and password security compliance behavior.

On the basis of the UTAUT framework, the following hypotheses are formulated in the context of password security compliance among healthcare employees:

Hypothesis 1: PE positively affects BI compliance with password security practices.
Hypothesis 2: EE positively influences BI to comply with password security practices.
Hypothesis 3: SI positively impacts BI to comply with password security practices.
Hypothesis 4: FC positively affects USE with respect to password security compliance.
Hypothesis 5: BI positively influences USE with respect to password security compliance.
Hypothesis 6: Gender moderates the relationships between 3 variables (PE, EE, and SI) and BI.
Hypothesis 7: Age moderates the relationships between 4 variables (PE, EE, SI, and FC) and BI.
Hypothesis 8: Experience moderates the relationships between 3 variables (EE, SI, and FC) and BI.

1.3. Conceptual framework

Figure 1 shows the conceptual framework of the study. The conceptual framework follows the UTAUT to assess password strength compliance. The framework outlines how the independent variables (PE, EE, SI, and FC) directly affect healthcare employees' intention (BI) to comply with password security practices. BI influences compliance with and usage of password security practices (USE). The moderating variables (age, gender, and experience) impact the strength of these relationships.

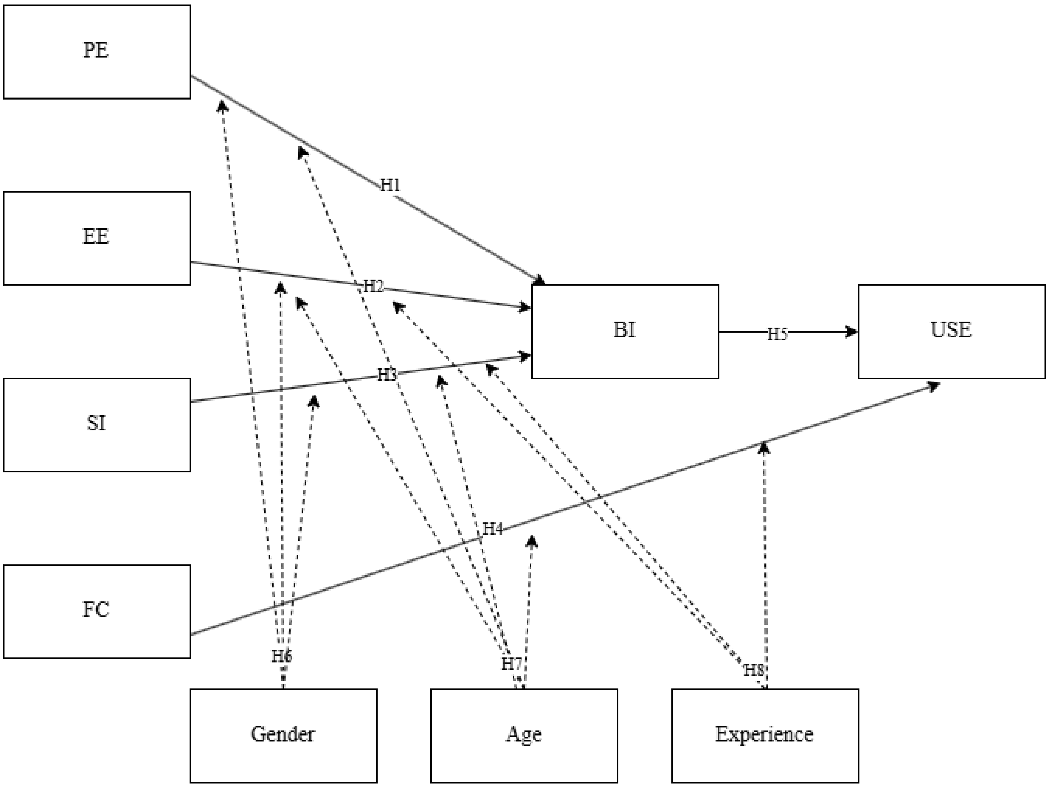

Figure 1 Proposed Conceptual Framework. *Note.* PE (performance expectancy), EE (effort expectancy), SI (social influence), FC (facilitated conditions), BI (behavioral intention), USE (actual usage or compliance).

2. Materials and Methods

This study uses the UTAUT as a framework to evaluate the effectiveness of password strength analysis tools in healthcare settings, specifically within a private hospital in Phuket. The methodology consists of several key steps, including selecting participants, data collection methods, analysis techniques, and ethical considerations.

2.1. Research design and setting

The research adopts a mixed-methods approach, combining quantitative and qualitative data collection techniques. This approach comprehensively explains healthcare users' acceptance of password security practices. The study aims to capture a broad spectrum of factors influencing user behavior and acceptance of password security practices. This approach allows us to examine the UTAUT constructs while providing contextual depth through qualitative feedback on user experiences and perceptions. The study assesses password strength compliance in healthcare settings via the UTAUT framework. The key variables are categorized into independent, dependent, and moderating variables. Independent variables are considered causal factors that influence dependent variables, typically represented on the left-hand side of an equation. According to the unified theory of acceptance and use of technology (UTAUT), four key independent variables influence two main dependent variables: behavioral intention (BI) and actual use (USE). These independent variables are performance expectancy (PE), defined as the degree to which healthcare employees believe that compliance with password strength requirements will enhance their job performance; effort expectancy (EE), referring to the perceived ease of using password strength compliance measures; social influence (SI), denoting the extent to which healthcare employees perceive social pressure to adhere to password security practices; and facilitating conditions (FCs), representing the availability of organizational support and resources for password security compliance.

The dependent variables are those that are influenced by other variables. According to the UTAUT, BI (healthcare employees' intention to comply with password security practices) and USE (actual compliance with password security practices among healthcare employees) are positioned on the right and far-right sides of the model, respectively. PE, EE, SI, and FC influence these variables. Three other variables, including age, gender, and experience, are moderating factors within the UTAUT model. These factors moderate the relationship between the independent and dependent variables, influencing the intention to comply with password security practices. The research is conducted within the confines of a private hospital located in Phuket. The hospital environment is exemplary for studying password security practices because of its reliance on advanced digital systems for managing sensitive patient data. A high demand for data security characterizes the hospital environment and represents modern healthcare institutions where digitalization plays a crucial role in daily operations.

2.2. Participants

The population utilized in this study consists of employees of a private hospital in Phuket, encompassing staff from three departments, including the clinical, semiclinical, and back-office sectors. The sample group comprises adult individuals. Using Yamane's formula with a margin of error of 5% and a total employee population of 1,000, the calculated sample size was approximately 286 (Yamane, 1973). The sample size used in the study exceeded this number to ensure greater accuracy and representation. The sampling method is simple random sampling, where sample units are randomly selected from the entire population. Data collection included personal information such as age, gender, education, occupation, and factors related to password security perceptions. This information is analyzed to identify and predict various factors influencing the adoption of password security practices.

The participants for this study were selected randomly to ensure that each hospital staff member had an equal chance of inclusion. This method minimizes selection bias and enhances the generalizability of the findings. The research team conducted the sampling process blindly and ensured that all departments within the hospital, including the clinical, semiclinical, and back-office sectors, were adequately represented. The inclusion criterion specified that participants must be current employees of the private hospital in Phuket, aged 20 years or older. This age criterion was established to ensure that respondents maturely understood password security practices. Both full-time and part-time staff were included, as their roles require familiarity with the hospital's IT systems and security practices. The exclusion criteria included contractors, temporary staff, and individuals under 20 years of age. These groups were excluded because they lacked full access to the hospital's IT systems or sufficient training on password security practices. Any employee who chose not to participate or withdrew consent at any stage was excluded to ensure that all data were collected from fully informed and willing participants.

2.3. Instruments

The primary instrument used for data collection was a structured questionnaire developed on the UTAUT model. This questionnaire included items measuring the PE, EE, SI, FC, BI, and USE constructs. The questionnaire will be validated through a pilot study with a small group of healthcare professionals to ensure its clarity and relevance (Venkatesh et al., 2003). Each construct was measured via validated scales adapted to the context of password management in healthcare. Furthermore, additional indirect variables from the UTAUT, including age, experience, and the voluntary nature of use, are considered. As the questionnaire required translation from English to Thai, three university lecturers fluent in both languages validated both versions to ensure semantic and syntactic consistency. This process was conducted before the Thai version was utilized in the research to guarantee its accuracy and equivalence to the original English version.

2.4. Procedure

The data collection was conducted over four months, including three monthly staff meetings. Advertisements inviting participation were placed at various locations within the hospital to maximize visibility and engagement. Potential respondents were directly approached during these monthly gatherings to increase participation rates. The participants were duly informed about their rights under ethical research standards. This included comprehensive information on their ability to withdraw from the study at any point without consequences and the option to opt out of completing the questionnaire. Furthermore, they were assured that the collected questionnaires contained no personally identifiable information, safeguarding their anonymity. All the responses were securely stored and retained for six months, after which they were permanently deleted, ensuring the confidentiality and security of the data.

The data collected from the surveys were analyzed via statistical software. Descriptive statistics summarize the demographic characteristics of the participants. In contrast, inferential statistics (e.g., regression analysis) test the relationships among UTAUT constructs regarding password security compliance. This survey may include age, gender, educational background, experience, the length of passwords used, and the inclusion of letters, numbers, and symbols in passwords. It also captures data on using the same password across multiple accounts. Notably, the data collected will be anonymized to ensure that they cannot be linked back to individual participants. The participants will be queried about the psychological and behavioral conditions associated with password security practices via a 7-point Likert scale. To assess construct validity and reliability, a confirmatory factor analysis (CFA) was performed on the data, using indicators such as the root mean square error of approximation (RMSEA), standardized root mean square residual (SRMR), comparative fit index (CFI), and Tucker–Lewis index (TLI) to evaluate the model's fit (Shi et al., 2019; Shi & Maydeu–Olivares, 2020).

The gathered data were examined via structural equation modeling (SEM) to evaluate the hypothesized connections between the UTAUT constructs. This method enables the simultaneous analysis of multiple relationships while assessing direct and indirect effects. Regression and path analysis were employed to examine the hypothesized relationships, following established practices in technology adoption research (Williams et al., 2015). The relationships between variables are examined through regression analysis and path analysis to explore how PE, EE, SI, and FC affect BI. Additionally, the influence of FC on USE is investigated. This involves statistically testing the significance of each relationship to confirm or refute the hypothesized links. For example, if PE and EE positively influence BI, hospital personnel are more likely to comply with password security practices if they perceive them as easy to use and beneficial.

2.5. Ethical considerations

The ethical approval process in research is a critical step to ensure that studies are conducted responsibly, respecting participants' rights, particularly in investigations assessing potential risks and benefits, which include considering possible harm or discomfort and planning mitigation strategies. This study, conducted under strict ethical guidelines approved by the Human Research Ethics Committee of Phuket Rajabhat University (PKRU2567/08) on April 29, 2024, with approval valid until April 28, 2025, adhered to ethical considerations such as obtaining informed consent, maintaining participant anonymity, and securely handling data. The participants were informed that they could withdraw without consequences, and all the data were securely stored and scheduled for destruction six months postanalysis to protect confidentiality.

3. Results

This section presents the results, highlighting the key constructs and their impact on compliance behaviors.

3.1. Sample characteristics

A total of 416 healthcare professionals participated in the survey, resulting in a response rate of 41.6%. The sample comprised 228 female respondents (55%) and 188 male respondents (45%). Demographic analysis revealed that nearly half of the participants were under 30 years of age (48.6%, n = 202), and a significant majority held a bachelor's degree (85.3%, n = 355). Data were collected through a pretested, self-administered questionnaire that captured sociodemographic information and critical constructs related to technology acceptance. The most significant proportion of respondents (56.7%, n = 236) had been employed at the hospital for 1 to 5 years. Most respondents (58.41%, n = 243) worked in clinical roles, reflecting the sample's clinical focus.

In terms of password security, most respondents used passwords with 8–10 characters (56.01%, n = 233), with nearly all incorporating uppercase letters (99.04%, n = 412), numbers (99.04%, n = 412), and special characters (97.60%, n = 406). Most (98.56%) follow recommended security practices by combining uppercase letters, numbers, and special characters in their passwords. Additionally, 97.83% of the respondents changed their passwords regularly, such as every 90 days, to maintain security. However, despite these strong security practices, 83.41% of the respondents used the same password across multiple accounts, highlighting critical vulnerability. While 97.12% of respondents have forgotten their passwords at some point, the majority (97.36%) know how to recover them, indicating a solid understanding of password recovery processes.

Nonetheless, some gaps in password security awareness remain. Notably, 15.63% of the respondents believe that weak passwords such as "password123" are acceptable, and 9.62% believe that writing passwords down on sticky notes is safe. Moreover, only 24.76% trust password managers to securely store passwords, reflecting a lack of familiarity or confidence in such tools. Although most respondents (96.39%) recognized the risks of transmitting passwords across unsecured networks, a small percentage (3.61%) remained unaware of this vulnerability. These findings suggest that while respondents generally follow password security practices, there are key areas where further education and awareness are needed to strengthen overall security behavior (Jerry-Egemba, 2023).

3.2. Descriptive results

The UTAUT model, as applied in this study, provides a comprehensive and well-fitting framework for understanding how PE, EE, SI, and FC influence healthcare employees' BI and USE of password security practices. The model's fit indices strongly align with the observed data. The SRMR value of 0.02 and RMSEA of 0.06, both within acceptable thresholds, suggest that the model's predictions closely match the actual responses, with the RMSEA's 90% confidence interval (0.05–0.14) indicating a reasonable level of model precision. Furthermore, the CFI (0.97) and GFI (1.00) values reflect excellent model fit, underscoring the robustness of the model in explaining password security compliance among healthcare professionals. The TLI (0.95) and RNI (0.97) further validate the model's appropriateness, emphasizing its ability to capture the complexity of factors influencing password security compliance. Table 1 presents the criteria for both good and acceptable fit indices.

3.3. Hypothesis testing results

Table 2 provides estimates from the SEM analysis, revealing the relationships between the UTAUT constructs and the outcomes of BI and USE. The estimate for the relationship between BI and USE is 0.69 ($p < 0.001$), indicating a strong positive effect. As employees' intentions to comply with password security increase, actual compliance also increases significantly. PE has the most significant impact on BI, with an estimate of 0.56 ($p < 0.001$). This suggests that when employees believe that complying with security measures will improve their job performance, their intention to comply increases substantially. EE also significantly influences BI, with an estimate of 0.26 ($p < 0.001$), reflecting that ease of use is crucial for encouraging compliance.

SI contributes positively to BI, with an estimate of 0.21 (p = 0.002), although it is less influential than PE and EE are. FC has a more minor but significant effect on USE, with an estimate of 0.12 (p = 0.036), indicating that organizational support is moderately crucial for ensuring actual compliance.

Table 1 Examples of fit indices used in SEM.

Fit Indices	Good Fit	Acceptable Fit	Research Framework
CFI	.95 ≤ CFI ≤ 1.00	.90 ≤ CFI < 1.00	0.97
GFI	.95 ≤ GFI ≤ 1.00	.90 ≤ GFI < 1.00	1.00
TLI	.95 ≤ TLI ≤ 1.00	.90 ≤ TLI < 1.00	0.95
RNI	.95 ≤ RNI ≤ 1.00	.95 ≤ RNI ≤ 1.00	0.97
RMSEA	0 ≤ RMSEA ≤ .05	.05 ≤ RMSEA ≤ .08	0.06
SRMR	0 ≤ SRMR ≤ .05	.05 ≤ SRMR ≤ .08	0.02

Note: CFI (comparative fit index), GFI (goodness-of-fit index), TLI (Tucker Lewis index), RNI (relative noncentrality index), RMSEA (root mean square error of approximation), SRMR (standardized root mean square residual).

Table 2 Parameter estimates from SEM analysis of the proposed model.

				95% Confidence Intervals			
Dep	Pred	Estimate	SE	Lower	Upper	β	p
USE	BI	0.69	0.04	0.60	0.78	0.60	***< .001
USE	FC	0.12	0.06	0.01	0.24	0.08	*0.036
BI	EE	0.26	0.04	0.18	0.33	0.29	***< .001
BI	PE	0.56	0.09	0.39	0.73	0.39	***< .001
BI	SI	0.21	0.07	0.08	0.34	0.19	**0.002

Note: * *p* < .05. ** *p* < .01. *** *p* < .001

Table 3 examines how gender moderates the relationships between UTAUT constructs and BI. Among female respondents, PE has a significant estimate of 0.49 (p < 0.001), EE has an estimate of 0.25 (p < 0.001), and SI has an estimate of 0.25 (p = 0.004). These results suggest that women are influenced by usefulness, ease of use, and social norms when forming their behavioral intentions to comply with password security policies. For male respondents, PE has an even more substantial influence, with an estimate of 0.69 (p < 0.001), and EE also remains significant, with an estimate of 0.27 (p < 0.001). However, SI is not essential for men (estimate 0.13, p = 0.233), indicating that peer or social pressures may have less influence on men. These results imply that interventions targeting women might benefit from emphasizing social norms, whereas ease of use and performance are more critical for men.

Table 3 Moderating effect of gender on UTAUT relationships.

					95% Confidence Intervals			
	Dep	Pred	Estimate	SE	Lower	Upper	β	p
F	BI	EE	0.253	0.0563	0.1424	0.363	0.2828	< .001
	BI	PE	0.493	0.1125	0.2723	0.713	0.3519	< .001
	BI	SI	0.247	0.0857	0.0789	0.415	0.2444	0.004
M	BI	EE	0.265	0.0545	0.1582	0.372	0.3082	< .001
	BI	PE	0.689	0.137	0.4209	0.958	0.4719	< .001
	BI	SI	0.13	0.1088	-0.0834	0.343	0.111	0.233

Note: * *p* < .05. ** *p* < .01. *** *p* < .001

Table 4 shows how age moderates the relationships between UTAUT constructs and BI or USE. For younger respondents (20–29 years), EE significantly influences BI, with an estimate of 0.32 (p = 0.005), and PE also has a strong effect, with an estimate of 0.50 (p = 0.019). SI is also significant, with an estimated value of 0.35 (p = 0.014), indicating that younger employees are more driven by social and performance factors. In contrast, for the oldest age group (50–59 years), FC has the most potent effect on USE, with an estimate of 0.40 (p = 0.002), meaning that older employees rely more on organizational resources and support to comply with password security practices. These results suggest that younger employees prioritize ease of use and performance, whereas older employees benefit more from available organizational resources.

Table 5 explores how experience moderates UTAUT relationships. For employees with 1–5 years of experience, EE significantly influences BI, with an estimate of 0.27 (p = 0.006), and SI also plays an important role, with an estimate of 0.27 (p = 0.038). This suggests that less experienced employees are more influenced by ease of use and peer behavior when forming intentions to comply with password security practices. As experience increases (e.g., 16–20 years), the impact of FC on USE decreases, with an estimate of 0.01 (p = 0.888), indicating that more experienced employees rely less on organizational support.

However, EE remains significant for experienced employees, with an estimate of 0.22 (p = 0.015), meaning that even experienced individuals value ease of use when adopting password security practices. This implies that training and resources may need to focus more on less experienced employees, while more experienced staff could benefit from usability improvements.

Table 4 Moderating effect of age on UTAUT relationships.

					95% Confidence Intervals			
	Dep	Pred	Estimate	SE	Lower	Upper	β	p
20 to 29 years	USE	FC	0.1783	0.1719	-0.1586	0.5152	0.0618	0.3
	BI	EE	0.322	0.1144	0.09772	0.5462	0.1914	0.005
	BI	PE	0.5024	0.2134	0.08424	0.9206	0.1959	0.019
	BI	SI	0.35	0.1424	0.07087	0.6291	0.203	0.014
30 to 39 years	USE	FC	0.1159	0.1337	-0.14626	0.378	0.082	0.386
	BI	EE	0.2327	0.0569	0.12115	0.3443	0.3587	< .001
	BI	PE	0.5801	0.1734	0.24034	0.9199	0.4818	< .001
	BI	SI	0.1068	0.1408	-0.16922	0.3829	0.1102	0.448
40 to 49 years	USE	FC	-0.0961	0.0707	-0.23475	0.0425	-0.0883	0.174
	BI	EE	0.1871	0.0571	0.07528	0.2989	0.2562	0.001
	BI	PE	0.6692	0.1106	0.45243	0.8859	0.585	< .001
	BI	SI	0.1794	0.0892	0.00455	0.3543	0.203	0.044
50 to 59 years	USE	FC	0.3994	0.1298	0.14492	0.6538	0.4046	0.002
	BI	EE	0.4038	0.1266	0.1557	0.6519	0.4128	0.001
	BI	PE	0.4669	0.1835	0.10726	0.8266	0.4559	0.011
	BI	SI	0.2305	0.1447	-0.05297	0.5141	0.2827	0.111

Note: * *p* < .05. ** *p* < .01. *** *p* < .001

Table 5 Moderating effect of experience on UTAUT relationships.

					95% Confidence Intervals			
	Dep	Pred	Estimate	SE	Lower	Upper	β	p
1 to 5 years	USE	FC	0.1193	0.1215	-0.1189	0.357	0.054	0.326
	BI	EE	0.2745	0.1008	0.077	0.472	0.1729	0.006
	BI	SI	0.2668	0.1289	0.0142	0.52	0.1749	0.038
6 to 10 years	USE	FC	0.2277	0.2176	-0.1988	0.654	0.1348	0.295
	BI	EE	0.3121	0.0801	0.1551	0.469	0.4966	< .001
	BI	SI	0.221	0.1853	-0.1422	0.584	0.2161	0.233
11 to 15 years	USE	FC	0.4381	0.3365	-0.2214	1.098	0.38	0.193
	BI	EE	0.1498	0.0389	0.0736	0.226	0.1875	< .001
	BI	SI	0.3873	0.0462	0.2968	0.478	0.4986	< .001
16 to 20 years	USE	FC	0.0135	0.096	-0.1747	0.202	0.0116	0.888
	BI	EE	0.2221	0.0913	0.0431	0.401	0.2608	0.015
	BI	SI	0.2506	0.1178	0.0196	0.482	0.2925	0.033

21 years and up	USE	FC	0.0393	0.076	-0.1097	0.188	0.0419	0.606
	BI	EE	0.2208	0.0826	0.0588	0.383	0.2791	0.008
	BI	SI	-0.1273	0.1641	-0.4489	0.194	-0.1374	0.438

Note: * *p* < .05. ** *p* < .01. *** *p* < .001

4. Discussion

This section discusses the key research findings, addresses the study’s limitations, and explores the implications for advancing behavioral science.

4.1. Discussion of the main results

The main findings of this study highlight the importance of the core constructs of the UTAUT framework, including PE, EE, SI, and FC, in shaping healthcare professionals’ behavioral intention (BI) to comply with password security practices and their actual compliance (USE). These results offer valuable insights into the factors influencing password security compliance, a critical issue in healthcare settings where data security is paramount owing to the sensitivity of patient information.

4.1.1. Performance expectancy (PE)

The analysis revealed that PE was the strongest predictor of healthcare professionals’ BI to comply with password security practices, with an estimate of 0.56 (p < 0.001). This finding suggests that when employees believe that complying with password security protocols will enhance their job performance or protect valuable healthcare data, they are significantly more inclined to adopt and adhere to such practices. In healthcare environments, where the security of patient data is not only a legal requirement but also integral to operational efficiency and patient safety, the perception that password security compliance enhances job performance becomes a key driver of behavior. This aligns with the literature on UTAUT, where PE is often the most significant predictor of intention in highly regulated industries such as healthcare, where performance and compliance are closely intertwined with professional responsibilities (Venkatesh et al., 2003). The strong relationship between PE and BI underscores the need for organizations to highlight the performance-related benefits of password security to healthcare professionals. Educational programs and policy enforcement mechanisms should emphasize how password security directly contributes to maintaining the integrity of patient data and supports the smooth functioning of health information systems. By doing so, institutions can reinforce the perception that these practices are not merely regulatory obligations but critical tools that facilitate employees’ professional tasks.

4.1.2. Effort expectancy (EE)

EE, with an estimate of 0.26 (p < 0.001), also significantly shaped healthcare professionals’ BI. EE reflects the perceived ease of complying with password security measures, which is particularly relevant in healthcare settings, where professionals are often under time constraints and face high workloads. If security measures are perceived as too complex or cumbersome, healthcare workers may avoid or neglect compliance. The significant positive relationship between EE and BI suggests that the more easily employees perceive password security practices, the more likely they are to comply with them. This finding is consistent with those of previous studies, which have shown that ease of use is a critical determinant of technology adoption, particularly in environments where operational efficiency is crucial (Davis, 1989). Healthcare organizations should focus on simplifying password security procedures to improve compliance. This might include implementing user-friendly password management tools, reducing the frequency of password changes, and providing clear guidelines for password creation. Moreover, organizations can offer training to improve staff familiarity with password management technologies, ensuring that security procedures do not interfere with patient care delivery. The significant role of EE in this study suggests that interventions aimed at reducing the perceived complexity of password security measures could lead to substantial improvements in compliance.

4.1.3. Social influence (SI)

SI also significantly affected BI, with an estimate of 0.21 (p = 0.002), although its influence was weaker than that of PE and EE. SI captures the extent to which individuals perceive that essential others (e.g., supervisors, colleagues, or organizational leaders) believe that they should comply with password security practices. In healthcare settings, where teamwork and hierarchical structures are standard, social norms and colleagues' behavior can significantly shape individual compliance. This finding suggests that employees are influenced by their peers’ and superiors’ behavior and expectations when deciding whether to follow password security protocols. This is consistent with previous studies that show that social influence can drive technology adoption in environments where group conformity and organizational culture play essential roles (Venkatesh & Davis, 2000). Healthcare organizations should cultivate a culture of security awareness to leverage SI to improve compliance.

Leadership should model proper security behavior, and peer influence should be harnessed through regular communication and training sessions, highlighting compliance's importance. Furthermore, recognition programs or peer-led initiatives that reward good security practices could reinforce the role of social influence in promoting adherence to security protocols.

4.1.4. Facilitating conditions (FCs)

FC had a modest but significant effect on actual password security practice (USE), with an estimated value of 0.12 ($p = 0.036$). FC refers to the availability of organizational support and resources that make it easier for employees to comply with password security practices. This includes access to training, technical support, and password management tools that facilitate adherence. The results suggest that while FC is not as influential as PE, EE, or SI in shaping BI, it plays a crucial role in determining whether employees will use the systems in place. This finding is consistent with the UTAUT literature, highlighting the importance of providing adequate support structures to encourage the use of new technologies or practices (Venkatesh et al., 2012). Healthcare organizations must ensure that sufficient resources are in place to support password security compliance. This could involve providing employees with easy-to-use password recovery systems, ensuring that technical support is readily available, and creating an environment where password security is prioritized. Since FC influences actual usage more than intention does, organizations should communicate the importance of compliance and ensure that the necessary tools and infrastructure are in place to facilitate compliance.

4.1.5. Moderating effects of gender, age, and experience

The results also indicate that gender, age, and experience significantly moderate the relationships between UTAUT constructs and BI or USE. Gender was found to moderate the effects of SI more strongly for women than for men, suggesting that women are more influenced by social expectations when complying with password security protocols. Age played a significant role in moderating the effects of EE, PE, and SI on BI, with younger employees being more influenced by ease of use and social factors. In comparison, older employees placed more emphasis on facilitating conditions. Experience also moderated the relationships, with less experienced employees being more influenced by SI and EE, whereas more experienced employees relied less on facilitating conditions and more on ease of use. These moderating effects suggest that tailored strategies are necessary to address different demographic groups' needs and motivations. For example, younger and less experienced employees might benefit from interventions emphasizing ease of use and peer support. In contrast, older or more professional employees might require more organizational support and resources. Gender-specific approaches might also be warranted, particularly in addressing the social dynamics influencing women's compliance with password security practices.

4.2. Limitations

This study has several limitations that should be acknowledged when contextualizing the findings. First, the reliance on self-reported data is prone to response bias, where participants may provide socially desirable responses, as demonstrated in prior cybersecurity studies (Fagan et al., 2017). This self-reporting could limit the accuracy of the results, as actual behavior may differ from reported behavior. Statistically, this bias can impact the validity of the regression models, potentially inflating relationships between variables such as PE and BI. Second, the study was conducted in a single private hospital in Phuket, which may limit the generalizability of the findings to other healthcare institutions, particularly public hospitals or those in different geographic or cultural contexts. The single-site nature of this study may limit generalizability, an issue commonly raised in cybersecurity and healthcare studies (Jerry-Egemba, 2023). The hospital's specific organizational and technological infrastructure may influence the observed relationships between FC and USE. Extending this research to a broader range of institutions would provide a more robust understanding of password security compliance across various healthcare settings. The study's cross-sectional design primarily precludes conclusions about causal relationships between the variables.

4.3. Contributions to multidisciplinary research

This study contributes to multidisciplinary research regarding technology adoption and password security compliance within healthcare settings. By applying the UTAUT to password strength compliance, this research enriches our understanding of how PE, EE, SI, and FC shape behavioral intentions. These constructs highlight their relevance in shaping secure password behaviors and advancing theoretical knowledge about the predictors of password security practices in highly regulated environments such as healthcare. This finding also supports previous findings that UTAUT constructs such as PE and EE are crucial to understanding technology adoption in regulated industries (Barchielli et al., 2021; Demsash et al., 2024. From a theoretical perspective, this study confirms the robustness of the UTAUT model in explaining password compliance behavior. This confirms the model by demonstrating how age and experience moderate vital relationships, with younger and less experienced employees being more influenced by PE and EE.

Further studies could examine how cognitive load and decision fatigue impact password security behaviors in high-stress environments such as healthcare (Holden & Karsh, 2010). Research could explore interventions to reduce the cognitive burden associated with frequent password changes and complex password requirements, potentially enhancing EE and increasing compliance rates. These findings emphasize the need for tailored cybersecurity training programs that address the specific needs of different employee demographics (Kuo et al., 2021). Policies should be designed to ensure compliance and foster an organizational culture that encourages password security practices through social influence and managerial support (O'Brien et al., 2020). The statistical results demonstrate that PE and EE are key predictors across all demographic groups, with more substantial effects observed in younger and less experienced employees. Policies should be adjusted to reflect the varying levels of influence of social and organizational factors on different age and experience groups (Humaidi & Balakrishnan, 2017).

5. Conclusions

This study comprehensively evaluates password security compliance within healthcare settings via the UTAUT framework. The findings confirm that PE, EE, and SI significantly influence healthcare employees' intentions to comply with password security practices. The study reveals that organizational support, through FC, positively impacts compliance with password security practices. Age and experience emerged as important moderating variables, with younger and less experienced employees showing a more substantial influence of PE and EE on their behavioral intentions. The significant moderation effects of age and experience underscore the need for tailored interventions, indicating that younger, less experienced employees are more responsive to effort and performance factors when complying with password security practices. This study contributes to the growing knowledge of password security in healthcare, offering theoretical insights and practical implications for improving password security compliance. Future research should focus on integrating cognitive and behavioral theories to explore further the complexities of technology adoption in high-stress environments such as healthcare (Huang et al., 2024).

Acknowledgment

We express our sincere gratitude to the executives and participants from the private hospital in Phuket for their invaluable cooperation and participation in the questionnaire. Their contributions were instrumental to the success of this study.

Ethical Considerations

I confirm that I have obtained all the consent required by the applicable law to publish any personal details or images of patients, research subjects, or other individuals used. I agree to provide the *Multidisciplinary Reviews Journal* with copies of the consent or evidence that such consent has been obtained if requested.

Conflict of Interest

The authors declare that they have no conflicts of interest.

Funding

This research did not receive any financial support.

References

AlQudah, A., Al-Emran, M., & Shaalan, K. (2021). Technology acceptance in healthcare: a systematic review. *Applied Sciences, 11*(22), 10537. https://doi.org/10.3390/app112210537

Aroms, E. (2012). *NIST special publication 800-63: Electronic authentication guideline*. CreateSpace Independent Publishing Platform.

Ayatollahi, H. & Shagerdi, G. (2017). Information security risk assessment in hospitals. *The Open Medical Informatics Journal, 11*(1), 37-43. https://doi.org/10.2174/1874431101711010037

Barchielli, C., Marullo, C., Bonciani, M., Rebecchi, A., Borrelli, F., Rapaccini, M., & Tani, M. (2021). Nurses and the acceptance of innovations in technology-intensive contexts: The need for tailored management strategies. *BMC Health Services Research*, *21*(639). https://doi.org/10.1186/s12913-021-06628-5

Breneol, S., Curran, J. A., Marten, R., Ndegwa, M., Drummond, J. H., Kiran, T., Ahmed, Z., & Wilson, K. (2022). Strategies to adapt and implement health system guidelines and recommendations: A scoping review. *Health Research Policy and Systems*, *20*(64). https://doi.org/10.1186/s12961-022-00865-8

Centers for Medicare & Medicaid Services (CMS), HHS (2006). Medicare program; revisions to payment policies, five-year review of work relative value units, changes to the practice expense methodology under the physician fee schedule, and other changes to payment under part B; revisions to the payment policies of ambulance services under the fee schedule for ambulance services; and ambulance inflation factor update for CY 2007. Final rule with comment period. *Federal register*, *71*(231), 69623–70251.

Davis, F. D. (1993). User acceptance of information technology: Ssystem characteristics, user perceptions and behavioral impacts. *International Journal of Man-Machine Studies, 38*(3), 475–487. https://doi.org/10.1006/imms.1993.1022

Demsash, A. W., Kalayou, M. H., & Walle, A. D. (2024). Health professionals' acceptance of mobile-based clinical guideline application in a resource-limited setting: Using a modified UTAUT model. *BMC Medical Education*, *24*(689). https://doi.org/10.1186/s12909-024-05680-z

Dickerson, J. E. (2022). Privacy, confidentiality, and security of healthcare information. *Anesthesia & Intensive Care Medicine, 23*(11), 740-743. https://doi.org/10.1016/j.mpaic.2022.08.014

Diel, S., Doctor, E., Reith, R., & Scheid, J. (2023). Examining supporting and constraining factors of physicians' acceptance of telemedical online consultations:

A survey study. *BMC Health Services Research, 23*(1128). https://doi.org/10.1186/s12913-023-10032-6

Ezugwu, A., Ukwandu, E., Ugwu, C., Ezema, M., Olebara, C., Ndunagu, J., Ofusori, L., & Ome, U. (2023). Password-based authentication and the experiences of end users. *Scientific African*, 21, e01743. https://doi.org/10.1016/j.sciaf.2023.e01743

Fagan, M., Albayram, Y., Khan, M., & Buck, R. (2017). An investigation into users' considerations toward using password managers. *Human-Centric Computing and Information Sciences, 7*(12). https://doi.org/10.1186/s13673-017-0093-6

Fernando, W. P. K., Dissanayake, D. A. N. P., Dushmantha, S. G. V. D., Liyanage, D. L. C. P., & Karunatilake, C. (2023). Challenges and opportunities in password management: a review of current solutions. *Sri Lanka Journal of Social Sciences and Humanities, 3*(2), 9-20. https://doi.org/10.4038/sljssh.v3i2.96

Govindarajan, U. H., Singh, D. K., & Gohel, H. A. (2023). Forecasting cyber security threats landscape and associated technical trends in telehealth using Bidirectional Encoder Representations from Transformers (BERT). *Computers and Security*, 133, 103404. https://doi.org/10.1016/j.cose.2023.103404

Holden, R. and Karsh, B. (2010). The technology acceptance model: its past and its future in health care. *Journal of Biomedical Informatics, 43*(1), 159-172. https://doi.org/10.1016/j.jbi.2009.07.002

Huang, W., Ong, W.C., Wong, M.K.F., Ng, E.Y.K., Koh, T., Chandramouli, C., Ng, C.T., Hummei, Y., Huang, F., Lam, C.S.P, & Tromp, J. (2024). Applying the utaut2 framework to patients' attitudes toward healthcare task shifting with artificial intelligence. *BMC Health Services Research, 24*(1). https://doi.org/10.1186/s12913-024-10861-z

Humaidi, N. and Balakrishnan, V. (2017). Indirect effect of management support on users' compliance behavior toward information security policies. *Health Information Management Journal, 47*(1), 17-27. https://doi.org/10.1177/1833358317700255

Inglesant, P. G., & Sasse, M. A. (2010). The true cost of unusable password policies: Password use in the wild. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (pp. 383–392). Association for Computing Machinery. https://doi.org/10.1145/1753326.1753384

Jamil, H., Zia, T., & Nayeem, T. (2021). User acceptance of password manager software: evidence from Australian microbusinesses. *Journal of Information Security and Cybercrimes Research, 4*(2), 148-158. https://doi.org/10.26735/kpob8473

Javaid, M., Haleem, A., Singh, R. P., & Suman, R. (2023). Toward insighting cybersecurity for healthcare domains: A comprehensive review of recent practices and trends. *Cybersecurity Applications*, 1, 100016. https://doi.org/10.1016/j.csa.2023.100016

Jerry-Egemba, N. (2023). Safe and sound: strengthening cybersecurity in healthcare through robust staff educational programs. *Healthcare Management Forum, 37*(1), 21-25. https://doi.org/10.1177/08404704231194577

Katsini, C., Fidas, C., Belk, M., Samaras, G., & Avouris, N. (2019). A human-cognitive perspective of users' password choices in recognition-based graphical authentication. *International Journal of Human-Computer Interaction, 35*(19), 1800-1812. https://doi.org/10.1080/10447318.2019.1574057

Kavrestad, J., Lennartsson, M., Birath, M., & Nohlberg, M. (2020). Constructing secure and memorable passwords. *Information & Computer Security, 28*(5), 701-717. https://doi.org/10.1108/ics-07-2019-0077

Ketikidis, P. H., Dimitrovski, T., Lazuras, L., & Bath, P. A. (2012). Acceptance of health information technology in health professionals: an application of the revised technology acceptance model. *Health Informatics Journal, 18*(2), 124-134. https://doi.org/10.1177/1460458211435425

Metallo, C., Agrifoglio, R., Lepore, L., & Landriani, L. (2022). Explaing users' technology acceptance through national cultural values in the hospital context. *BMC Health Services Research, 22*(1). https://doi.org/10.1186/s12913-022-07488-3

Nair, A., & Greeshma, M. R. (2023). *Mastering information security compliance management: A comprehensive handbook on ISO/IEC 27001:2022 compliance*. Packt Publishing.

O'Brien, N., Graß, E., Martin, G., Durkin, M., Darzi, A., & Ghafur, S. (2020). Developing a globally applicable cybersecurity framework for healthcare: a delphi consensus study. *BMJ Innovations, 7*(1), 199-207. https://doi.org/10.1136/bmjinnov-2020-000572

Shi, D. & Maydeu-Olivares, A. (2020). The effect of estimation methods on SEM fit indices. *Educational and Psychological Measurement, 80*(3), 421–445. https://doi.org/10.1177/0013164419885164

Shi, D., Lee, T., & Maydeu-Olivares, A. (2019). Understanding the model size effect on SEM fit indices. *Educational and Psychological Measurement, 79*(2), 310–334. https://doi.org/10.1177/0013164418783530

Sullivan, N., Tully, J., Dameff, C., Opara, C., Snead, M., & Selzer, J. (2023). A national survey of hospital cyber attack emergency operation preparedness. *Disaster Medicine and Public Health Preparedness*, 17, e363. https://doi.org/10.1017/dmp.2022.283

Uwizeyemungu, S., Poba-Nzaou, P., & Cantinotti, M. (2019). European hospitals' transition toward fully electronic-based systems: do information technology security and privacy practices follow? *Jmir Medical Informatics, 7*(1), e11211. https://doi.org/10.2196/11211

Venkatesh, V., Morris, M., Davis, G., & Davis, F. (2003). User acceptance of information technology: toward a unified view. *Mis Quarterly, 27*(3), 425–478. https://doi.org/10.2307/30036540

Wazid, M., Das, A. K., Mohd, N., & Park, Y. H. (2022). Healthcare 5.0 security framework: applications, issues and future research directions. *IEEE Access*, 10, 129429-129442. https://doi.org/10.1109/access.2022.3228505

Williams, M. D., Rana, N. P., & Dwivedi, Y. K. (2015). The unified theory of acceptance and use of technology (UTAUT): A literature review. *Journal of Enterprise Information Management, 28*(3), 443–488. https://doi.org/10.1108/JEIM-09-2014-0088

Yamane, T. (1973). *Statistics: An Introductory Analysis*. 3rd Edition, Harper and Row, New York

Zimmermann, V., Marky, K., & Renaud, K. (2022). Hybrid password meters for more secure passwords – a comprehensive study of password meters including nudges and password information. *Behavior and Information Technology, 42*(6), 700-743. https://doi.org/10.1080/0144929x.2022.2042384