Archives of Public Health

RESEARCH Open Access

Decoding privacy concerns: the role of perceived risk and benefits in personal health data disclosure

Havva Nur Atalay[1*] and Şebnem Yücel[2]

Abstract

Background Personal health data is crucial for effective medical care, personalized treatment, and health monitoring. It enables accurate diagnosis, efficient treatment plans, and informed healthcare decisions. Personal health data should be protected to ensure patient privacy, prevent misuse or unauthorized access, and maintain trust in healthcare systems, thereby safeguarding individuals' sensitive information from potential harm or exploitation. Therefore, this study aimed to investigate whether perceived risk and perceived benefits have mediating roles in the relationships among individuals' personal health information disclosure behaviour, perceived control, and privacy concerns.

Method The population of the study consisted of individuals living in the provinces of Izmir, Konya and Adana. The sample of the study consisted of individuals who were reached through a convenience sampling method. The scales for privacy concerns, perceived control, perceived risk, perceived benefits and information disclosure behaviour were used in the study. Cronbach's alpha and the AVE were calculated, and a confirmatory factor analysis was performed. A path analysis was performed using the structural equation model to test the hypotheses.

Results The analysis revealed a significant negative relationship between individuals' personal health data disclosure behaviour and their privacy concerns. However, perceived risk and perceived benefit did not mediate this relationship. Additionally, a significant positive relationship was found between individuals' behaviour of disclosing their perceived control and personal health data, with perceived risk and benefits playing a mediating role in this relationship.

Conclusion The study concluded that as individuals' concerns about sharing personal health data increase, they are less likely to share these data. It was also found that perceived risk and perceived benefit mediate this relationship. Additionally, higher perceived risk intensifies privacy concerns, further discouraging data sharing, while perceived benefits can mitigate these concerns, promoting greater willingness to disclose health information.

Keywords Personal health data, Perceived risk and benefit, Privacy concern, Perceived control, Information disclosure behaviour

*Correspondence:
Havva Nur Atalay
hatalay@bandirma.edu.tr
[1]Faculty of Health Sciences, Department of Health Management, Bandırma Onyedi Eylül University, Balıkesir, Turkey
[2]Faculty of Health Sciences, Department of Health Management, Selçuk University, Konya, Turkey

Text box 1. Contributions to the literature

This study integrates the dimensions of perceived control, privacy concerns, and health information disclosure, addressing a gap in the health literature where these factors have not been examined together.

It reveals the mediating roles of perceived risks and benefits in the relationship between privacy concerns and health information disclosure behavior.

By providing new insights into the factors influencing health data disclosure, this research contributes to the development of more effective public health policies and practices.

The findings suggest the need for further research into other potential mediators in the privacy-disclosure relationship within healthcare.

Introduction

Personal data, whose management belongs to both the individual and the state through law [1], is information that belongs to and identifies the individual. Personal health data, on the other hand, are considered special data within this information. The information obtained about the individual health of the individual constitutes personal health data. Because these data have commercial value, they are attractive targets for marketers, identity thieves and many organizations in many sectors [2]. Therefore, the disclosure of personal health data online in electronic media is considered risky for many reasons, such as cyberattacks, malicious software developers, and the presence of individuals or institutions who want to gain financial resources [3]. According to Bansal et al. [4], in healthcare, when personal health information is disclosed online, it can be misused or accessed without permission. In addition, the risks of information leakage and violations of privacy and security that may occur while personal and clinical information is collected, used and stored by hospitals are very important issues [5]. Privacy is viewed as a dynamic concept, "in the sense that it is multidimensional, flexible, location dependent, and changes according to life experience" [6].

Concerns about information privacy involve controlling access to information, ensuring the security of information exchange, and verifying that those collecting the information adhere to established regulations [4]. Therefore, one of the main factors of privacy is the perceived level of control [7]. Perceived control is the belief that one's actions, efforts, and choices can influence changes in the environment [8] and one's belief about the level of completion of a particular action [9]. Perceived risks for privacy are related to the uncertainty that arises from the potential malicious use of personal data [10, 11]. With respect to individuals' information disclosure behaviour, it is expected that the perception of risk is the lowest and that the perception of benefits is high [12].

Perceived benefits are related to the benefits that will occur after individuals engage in information disclosure. The integration of perceived risks and benefits is fundamental to privacy account theory. According to this model, individuals are more inclined to disclose information when they perceive minimal risks and maximum benefits [13]. Smith et al. [14] determined the antecedents, privacy concerns and outcomes of the disclosure of personal data by using the macro APCO (Antecedents, Privacy, Concerns, Outcomes) model. APCO brings together the body of knowledge on information privacy by integrating key factors explored in various studies, commencing with the examination of privacy apprehensions, which is the most frequently investigated element within this domain [15]. Dinev et al. [16] proposed the macro APCO model, in which individuals are affected by external factors while sharing their personal data, and this influence causes behavioural changes by creating privacy concerns. In this study, in addition to the APCO model, the perceived control of individuals was measured, and their behaviours related to personal health data disclosure were examined. It is thought that examining the APCO model in the context of personal health data disclosure will contribute to the literature. Therefore, in this study, the mediating role of perceived risk and perceived benefit in the relationship between individuals' health information disclosure behaviour, privacy concerns and perceived control was investigated.

Conceptual framework

The conceptual framework of this study is based on the examination and development of previous studies related to individuals' intention to share personal health data. The mediating role of perceived risk and perceived benefits in the relationships of perceived control, privacy concern and behaviour of personal health data disclosure are included, in the present hypothesized model.

Information disclosure behaviour

The information disclosure behaviour refers to the likelihood of individuals sharing their information with a person or platform other than themselves [6]. The individual decision process regarding data disclosure is influenced by many factors. Incomplete knowledge, limited rationality, and systematic psychological deviations from rationality demonstrate that the assumption of perfect rationality may not fully capture the complexities of an individual's privacy-sensitive behaviour. Factors such as incomplete information, externalities, information asymmetries, risks, and uncertainties influence individuals' intentions regarding information disclosure [17]. Across various domains of personal data disclosure, studies from the past to the present have consistently emphasized the overarching privacy concern of consumers,

which is defined as an individual's inclination to be concerned about the privacy of their information [18–21]. In a study conducted by Chen [22], it was concluded that the increase in privacy concerns of individuals reduces individuals' behaviour of information disclosure. At the same time, another study by Zlatolas et al., [23] argued that privacy concerns and perceived benefits have a direct impact on individuals' behaviour of information disclosure.

Privacy concern

In today's digital landscape, competitive strategies rely increasingly on the utilization of vast quantities of processed data. Information practices in which this data, which provides value to organizations, creates privacy concerns for individuals [24–26]. In other words, the connectivity of wired and wireless network platforms has resulted in an expansion of data sources and easier access to personal information [27] and accordingly, individuals' privacy concerns have increased. Privacy concern is the concern of individuals regarding the information privacy practices of institutions. Concern for privacy reflects the perceived likelihood of privacy breaches and individuals' responses to expected losses during privacy breaches [28]. Privacy concern is defined as the need to protect against unwanted communication and misuse of personal information [29]. Confidentiality of personal health data means a set of rules that limit the permission to share information transferred between the patient and the physician. Furthermore, privacy in health information pertains to an individual's entitlement to control the sharing of their health-related data [30]. The concern for the privacy of health information may even cause individuals to avoid health services in sensitive areas [4]. The fact that there are confidentiality violations in the sharing of personal health data also undermines the trust of individuals in healthcare professionals.

H1: Privacy concern is negatively related to the behaviour of information disclosure.

Perceived control

The focus of the concept of control is that consumers decide how much information they want to share, how they want others to perceive it, or how they should share it themselves [31]. At this point, the sense of control can be a factor that increases the individual's capacity and competence to handle consequences [9, 32, 33]. Data may be shared between organizations provided it is used for legitimate health purposes. The privacy and security measures of the organization that receives the data should be equivalent to those that collect the data [34]. At this point, control creates a sense of security and creates a sense of trust without risks [7]. Trust is defined as the absence of control over the actions of another party, regardless of its ability to monitor or control the other party, based on the expectation that one party will take a particular action that is important to the other party [35].

Confidence in health services is high due to information asymmetry. The personal information obtained during this relationship between the physician and the patient should not be shared with others unless the patient is aware of the sharing of his/her information [36]. Li et al. [27], suggest that individuals who perceive a high level of control over their data believe they possess greater authority over the sharing and subsequent utilization of their personal information. On the contrary, individuals with high privacy risk beliefs tend to be more cautious about the potential loss of control over their personal information. Das and Teng [37] propose that control can be viewed as a crucial mechanism for fostering trust in cooperative behaviour among involved parties. Perceived control handled in this way helps to spread an atmosphere of trust in a platform [38]. Thus, perception of high information control mitigates perceived risks and positively increases their individuals' information disclosure behaviour [39]. As a result, based on the literature, it is thought that individuals will share the data they want when they have control over their personal data.

H2: Perceived control is positively related to the behaviour of information disclosure.

Perceived risk

Perceived risk can be thought of as a combination of uncertainty about the possible consequences of a behaviour and the possible harms of these consequences [40]. Therefore, the perceived risk is related to the possible problems that may arise due to the termination of the user's or third parties' access to their personal information [19, 31]. According to Boshoff et al., [41] perceived risks are seen as a means of uncertainty about the potential consequences of a behaviour and the possible negativity of these consequences. Accordingly, it is related to privacy risks and uncertainty caused by the possibility of personal data misuse [10]. In health services, personal health data recorded during diagnosis, examination and treatment can be easily analyzed, distributed and reused. Therefore, in addition to the positive consequences of this convenience, individuals perceive a relatively high risk of using it for unrelated purposes without their knowledge or consent [42]. For example, cloud service providers can abuse data to sell it to third parties. Such privacy attacks affect users' trust and make them skeptical about storing sensitive data [43].

H3: Perceived risk is positevly related to the privacy concern.
H4: Perceived risk mediates the relationship between privacy concern and information disclosure behaviour.
H5: Perceived risk mediates the relationship between perceived control and information disclosure behaviour.

Perceived benefit

Perceived benefits are the sum of the benefits and satisfactions of individuals that satisfy their needs and wants. This is the perception of what individuals gain after sharing data [44]. At the same time, perceived benefit forms a fundamental part of an individual's choices [12]. Perceived benefit is also defined as being aware of the gain that individuals will gain if they share their personal information [20, 45]. Park and Chai [46] have examined the concept of value in relation to the benefits of sharing personal data. At this point, it should be noted that individuals tend to share data that they believe will create value and benefit. Hence, it is hypothesized that perceived benefits and risks play a pivotal role in the relationships between individuals' behaviour of information disclosure, perceived control, and privacy concerns.

H6: Perceived benefit is positively related to the perceived control.

H7: Perceived benefit mediates the relationship between privacy concern and behaviour of information disclosure.

H8: Perceived benefit mediates the relationship between perceived control and behaviour of information disclosure.

Research methodology

The purpose of the research part of the study is to investigate the mediating role of perceived risk and perceived benefit in the relationship between information disclosure behaviour and privacy concerns and perceived control. In line with the literature, the study seeks to answer the following questions:

1. What is the relationship between information disclosure behaviour, privacy concerns, perceived control, perceived risks and perceived benefits?
2. What is the role of perceived benefit and perceived risk in the relationship between information disclosure behaviour and privacy concern and perceived control?

This study employed a cross-sectional design and proposed a hypothesized model to elucidate privacy concerns, perceived control, risk, benefits, and the disclosure of personal health information among individuals. Model fitness was addressed by testing hypothetical paths (Fig. 1). According to Fig. 1, there are significant relationships between privacy concerns and the intention to share data as well as between perceived control and the intention to share data. Additionally, perceived risk and perceived benefit play a mediating role in these relationships.

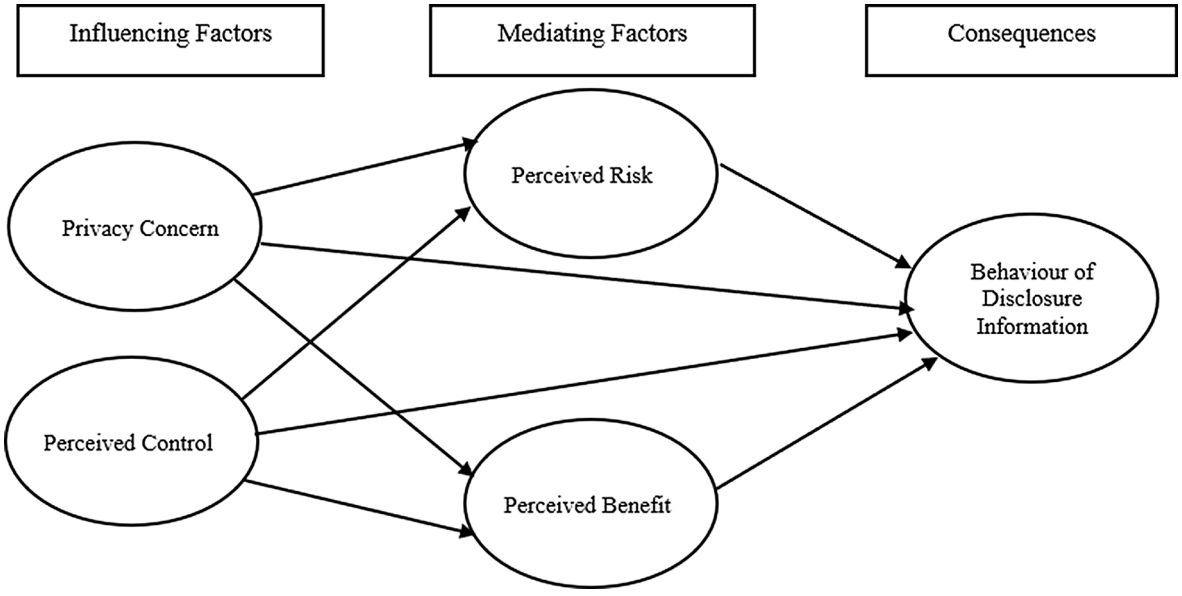

Fig. 1 Conceptual model of the research exploring privacy concerns, perceived control, risk, benefit and personal health information disclosure

Study population and sample

The research was conducted using the random sampling method in the province of Konya from the Central Anatolian Region, in the province of Izmir from the Aegean Region, and in the province of Adana from the Mediterranean Region. Therefore, the population of the research consisted of individuals living in the provinces of Izmir, Konya and Adana. According to the random sampling method, all units in the main population should be homogeneous, and the selection of one individual should not affect the probability of another being selected [47]. The research sample size was determined based on the principle that it should be at least five to ten times the number of items in validity and reliability studies. Consequently, although the sample size was initially set at 600 individuals, the research sample ultimately comprised 635 individuals who were reached through a convenience sampling method [47–49]. The number of individuals to be reached from each city in the study was determined using the stratified sampling method. According to this sampling method, the population is divided into distinct subgroups or strata, and a specific proportion (stratum quota) of individuals is included in the sampling from each stratum [48–50]. In this study, the population was divided into groups according to size (Table 1).

The number of individuals to be reached from each province in the research was determined using the stratified sampling method. According to this method, the population is divided into different subgroups, and a certain percentage of individuals (quota) from each group is included in the sample. The populations of Izmir, Konya, and Adana are given in Table 1. First, the populations of these provinces were summed, and quota ratios were determined by dividing the population of each province by the total population. Then, the previously determined sample size of 600 people was multiplied by the percentages to determine the minimum number of individuals from each province to be included in the study. The survey was organized on Google Forms and delivered to the participants via various social platforms (Twitter, Instagram, Facebook, WhatsApp, LinkedIn). In this context, the study was conducted using the data of 635 participants who agreed to participate in the study and who answered the survey questions completely.

Data collection tools

The scales for privacy concerns, perceived control, perceived risk, perceived benefits and behaviour related to information disclosure were used in this study.

Privacy concern scale The Privacy Concern Scale was developed and tested for validity and reliability by Yuan Sun, Fand & Hwang [51]. The scale consists of 3 items. The statements are suitable for the 5-point Likert scale of 1-strongly disagree and 5-strongly agree. The internal consistency coefficient (Cronbach's alpha) of the scale is 0.90.

Perceived Control Scale The Perceived Control Scale developed by Li, Luo, Zhang & Xu [52], whose validity and reliability tests were performed, consists of 3 items. The statements were answered on a 5-point Likert scale ranging from 1-strongly disagree to 5-strongly agree. The internal consistency coefficient of the scale is 0.92.

Perceived risk scale The Perceived Risk Scale developed by Xu et al. [6] for Position Sensitive Marketing Measurement consists of 3 items. The statements are 7-point Likert-type, ranging from 1-strongly disagree to 7-strongly agree. The internal consistency coefficient of the scale is 0.94, indicating high reliability.

Perceived benefit scale The Perceived Benefit Scale developed by Xu et al. [6] for Position-Sensitive Marketing Measurement consists of 3 items. The statements are 7-point Likert-type. The internal consistency coefficient of the scale is 0.91.

Information disclosure behaviour scale The Scale developed by Xu et al., [6] for Position Sensitive Marketing Measurement and for which validity and reliability tests were conducted, was used to measure individuals' intention to disclose data. The scale consists of 3 items. The statements are suitable for a 7-point Likert scale. The internal consistency coefficient of the scale is 0.86.

Data collection method

The study data were collected online via Google Forms between June 2021 and January 2022. After receiving approval from the ethics committee and obtaining

Table 1 Distribution of the Sample size by City based on stratified sampling method for the study conducted in Adana, Izmir, and Konya cities in Türkiye (January–May 2022)

Province	Population of Province	Determining Quota Ratios		Sample size
İzmir	4.367.251	4.367.251/8.837.565 = 0,50	%50	600*0,50 = 300 people
Konya	2.232.374	2.232.374/8.837.565 = 0,25	%25	600*0,25 = 150 people
Adana	2.237.940	2.237.940/8.837.565 = 0,25	%25	600*0,25 = 150 people
Total	**8.837.565**		**%100**	**600**

Note The relevant population data were obtained from the population census information of the Turkish Statistical Institute

Table 2 Normal distribution values of the scales used in the study

Scales used in the study	Skewness	Kurtosis
Privacy Concern Scale	0,050	-0,555
Perceived Control Scale	-0,324	-0,235
Perceived Risk Scale	-0,020	-0,717
Perceived Benefit Scale	-0,591	-0,124
Information Disclosure Behaviour Scale	-0,485	-0,354

Table 3 Goodness of fit indices for the structural model of the study

Goodness of Fit Values	Acceptable Fit Values	Good Fit Valuess	Model Values
CMIN/DF	CMIN /DF < 5	CMIN /DF < 3	2,759
RMSEA	0,05 < RMSEA ≤ 0,10	0 ≤ RMSEA ≤ 0,05	0,947
GFI	0,85 ≤ GFI < 0,90	0.90 ≤ GFI ≤ 1.00	0,965
AGFI	0,85 ≤ AGFI < 0,90	0.90 ≤ AGFI ≤ 1.00	0,926
CFI	0,95 ≤ CFI < 0,97	0,97 ≤ CFI ≤ 1.00	0,949
NFI	0,90 ≤ NFI < 0,95	0,95 ≤ NFI ≤ 1.00	0,53

institutional permission, the survey was distributed to participants through various social platforms, such as Twitter, Instagram, Facebook, WhatsApp, and LinkedIn. The survey consisted of several components, including an informed consent form, a demographic data section, and scales measuring privacy concern, perceived control, perceived risk, perceived benefit, and information disclosure behaviour.

Data analysis

For the analysis of the research data, descriptive statistics (standard deviation, mean) were calculated using the SPSS 26.0 program. Cronbach's alpha was calculated with the SPSS 26.0 program for reliability analysis. Confirmatory Factor Analysis (CFA) was conducted with the AMOS Graphics program for validity analysis. The study employed Structural Equation Modeling (SEM). SEM was used to test the hypotheses. In other words, SEM was used to verify structural theory. Skewness and kurtosis values were examined to determine the fit for a normal distribution.

Findings

According to the sociodemographic data, 43.1% (274) of the participants were female, while 56.9% (361) were male. The majority of participants were individuals aged 22 and under, comprising 38.6% (245) of the sample. Most participants were university graduates (55.7% (354)), followed by high school graduates (20.2% (128)), graduate degree holders (17.5% (111)), and primary school graduates (6.6% [42]). In this research, we investigated whether the scales were suitable for a normal distribution. The data obtained are shown in Table 2.

Skewness and kurtosis values were examined to determine the fit for a normal distribution. If these values are between −1 and +1, it can be said to fit the normal distribution [53]. In this respect, Table 2 shows that the scales conform to a normal distribution.

Findings regarding the validity and reliability of the scales

The validity and reliability of the scales used in the study were examined by CFA. The goodness of fit values for the scales are indicated in Table 3.

In the literature, if the $\chi 2/df$ ratio is <5, it is acceptable, and if it is <3, it is a good fit. The RMSEA showed good agreement when $0 \leq RMSEA \leq 0.05$ and acceptable agreement when $0.05 < RMSEA \leq 0.10$ [54]. A range of GFI values of $0.90 \leq GFI \leq 1.00$ represents good fit, and a range of $0.85 \leq GFI < 0.90$ represents acceptable fit [55, 56]. The AGFI value is defined as good agreement between $0.90 \leq AGFI \leq 1.00$ and acceptable agreement between $0.85 \leq AGFI < 0.90$ [55]. For the CFI, $0.97 \leq CFI \leq 1.00$ indicates good agreement, and $0.95 \leq CFI < 0.97$ indicates acceptable agreement [57]. The NFI value is expressed as a good fit between $0.95 \leq NFI \leq 1.00$ and an acceptable fit between $0.90 \leq NFI < 0.95$ [58].

In the model created within the scope of the research, 5 different scales were used. The reliability of the scales was calculated by Cronbach's alpha and the AVE. The data obtained are given in Table 4. Based on the data presented in Table 4, the scales were deemed reliable, as both the Cronbach's alpha coefficients and the AVE values fell within acceptable ranges, indicating reliability. CFA was applied to the scales, and acceptable fit values were reached in the initial version (goodness-of-fit statistics: $\chi 2/df = 2.759$, NFI = 0.947, CFI = 0.965, AGFI = 0.926, GFI = 0.949, RMSEA = 0.053). For the model to reach good fit values, the proposed covariance between the error terms was created and the model was rerun. Accordingly, a model with good fit values was obtained (goodness-of-fit statistics: $\chi 2/df = 2.196$, NFI = 0.958, CFI = 0.977, AGFI = 0.943, GFI = 0.961, RMSEA = 0.043). The CFA model made with the AMOS Graphics program is shown in Fig. 2.

In this research, the relationships between the variables were investigated by correlation analysis. The results are shown in Table 5.

According to Table 6, there is a low-level negative correlation between information disclosure behaviour and both privacy concerns (r=-0.15; $p<0.01$) and perceived risk (r=-0.13; $p<0.01$). Furthermore, a moderately significant positive correlation was detected between information disclosure behaviour and both perceived control (r=0.37; p 0.01) and perceived benefits (r=0.52; $p<0.01$). A weak negative correlation was observed between perceived benefits and both privacy concerns (r=-0.12; $p<0.01$) and perceived risk (r=-0.08; $p<0.05$).

Table 4 Confirmatory factor analysis results of the research model exploring privacy concerns, perceived control, perceived risk and benefit, and personal health information disclosure

Items	STD estimate*	STD estimate*	Estimate	SE	t Value (CR = estimate/SE)	Cronbach Alpha	AVE	Mean	Std. Deviation
Privacy Concern						0,823	0,51		
1.	0,632	0,644	1,000					3,01	1,125
2.	0,736	0,763	1,279	0,083	15,321			3,01	1,215
3.	0,810	0,755	1,289	0,085	15,085			2,89	1,237
4.	0,761	0,763	1,201	0,085	14,152			3,12	1,249
Perceived Control						0,824	0,49		
1.	0,577	0,576	1,000					3,84	1,059
2.	0,759	0,761	1,476	0,122	12,052			3,31	1,185
3.	0,729	0,728	1,385	0,116	11,970			3,51	1,162
Perceived Risk						0,861	0,68		
1.	0,803	0,804	1,000					3,86	1,661
2.	0,851	0,850	1,149	0,050	22,943			4,20	1,804
3.	0,813	0,813	1,053	0,048	21,877			3,89	1,730
Perceived Benefit						0,807	0,56		
1.	0,668	0,583	1,000					5,42	1,513
2.	0,839	0,770	1,202	0,075	15,928			5,61	1,377
3.	0,796	0,856	1,374	0,107	12,870			5,43	1,416
Information Disclosure Behaviour						0,862	0,68		
1.	0,831	0,832	1,000					5,04	1,624
2.	0,904	0,902	1,174	0,048	24,552			4,92	1,756
3.	0,740	0,741	0,930	0,046	20,418			4,82	1,695

* Factor load for all factors $p<0.001$

Additionally, a moderately significant positive correlation was found between perceived benefits and perceived control ($r=0.44$; $p<0.01$). Furthermore, a strong positive relationship was observed between perceived risk and privacy concerns ($r=0.70$; $p<0.01$). Additionally, there was a weak negative correlation between perceived risk and perceived control (r=-0.17; $p<0.01$) and a weak negative correlation between perceived control and privacy concerns ($r=0.19$; $p<0.01$). In this research, the structural equation model was applied with the AMOS Graphics program to test the hypotheses.

In the first stage, the relationship between privacy concerns and information disclosure behaviour was determined by performing path analysis alone. As a result of this analysis, the path coefficient between privacy concerns and information disclosure behaviour was found to be -0.29. This result corresponds to the first of the mediator variable results and indicates that there may be a relationship. In addition, the relationship between perceived control and information disclosure behaviour was determined by performing path analysis alone. As a result of this analysis, the path coefficient between perceived control and information disclosure behaviour was found to be 0.93. This result corresponds to the first of the mediator variable results and indicates that there may be a relationship.

Path analysis was conducted to determine the role of perceived benefits and risks in the relationships between privacy concerns and perceived control and information disclosure behaviour. The path model of the analysis is given in Fig. 3. The analysis revealed a significant relationship between perceived risk and privacy concerns (1.15, $p<0.01$), there is no between privacy concerns and information disclosure behaviour (-0.03, $p<0.05$). However, no significant relationships were found between perceived risk and information disclosure behaviour (-0.03, $p>0.05$), between privacy concerns and perceived benefits (-0.06, $p>0.05$). The bootstrap method is used to examine the mediation effect in contemporary approaches. According to this method, if there is no 0 (zero) between the bootstrap upper and lower values, the mediation effect can be mentioned, while if it is 0 (zero), there is no mediation effect (Hayes 2018). According to the bootstrap values of the model (lower value=-0.215; upper value=0.120), perceived risk and perceived benefit don't have a mediating role in the relationship between privacy concerns and information disclosure behaviour (-0.203, 0.134). A significant relationship was found between the perceived benefit and information disclosure behaviour (0.67, $p<0.01$) and perceived control (0.73, $p<0.01$) and between the perceived risk and information disclosure behaviour (-0.03, $p<0.01$) and perceived

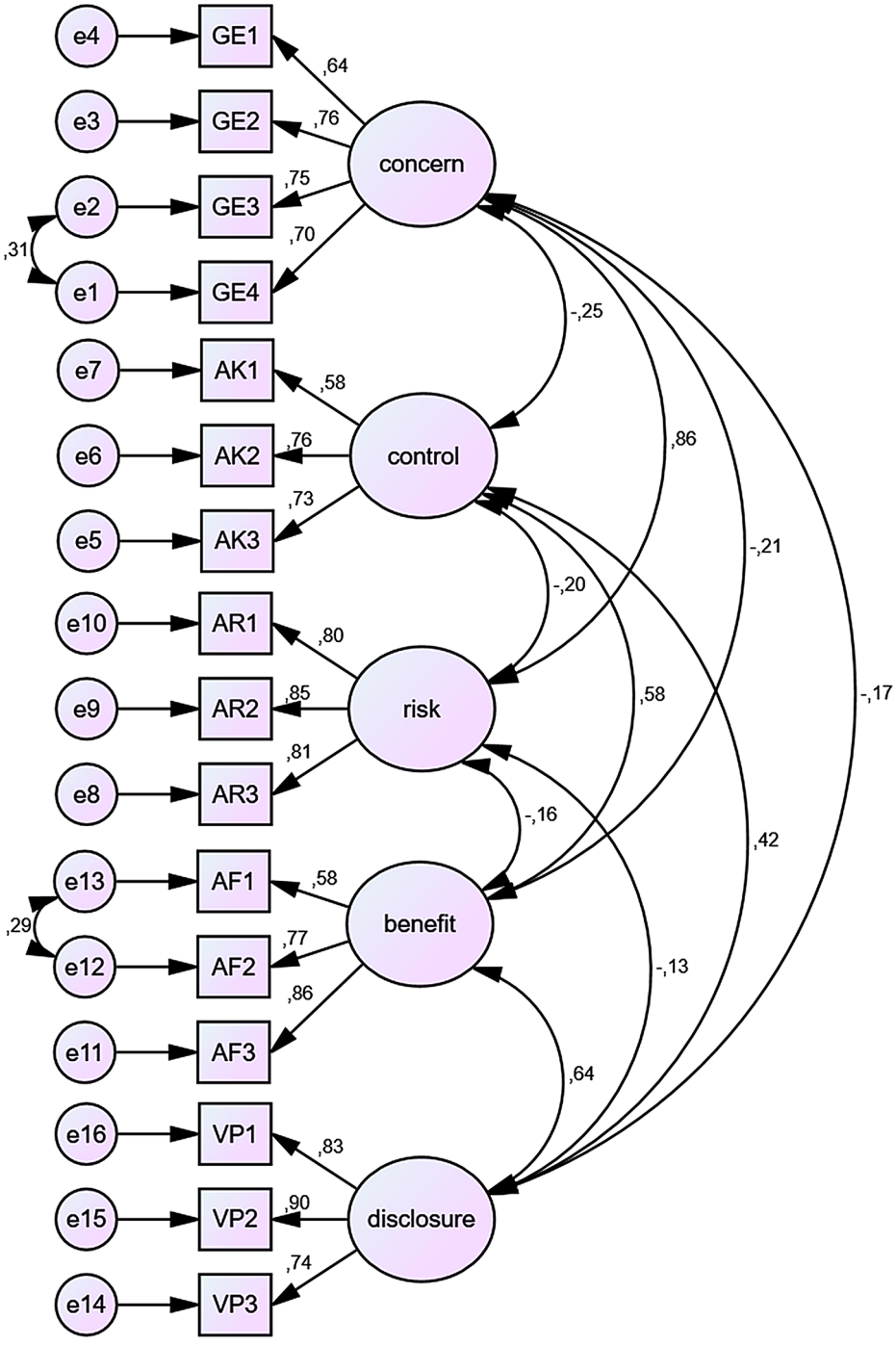

Fig. 2 Confirmatory factor analysis of the research model exploring privacy concerns, perceived control, perceived risk and benefit, and personal health information disclosure

control (-0.05, $p<0.01$). In addition, although there was a significant relationship between perceived control and information disclosure behaviour in the first stage, this relationship was not found in the model (0.16, $p>0.05$). In this case, there is a mediating effect on the relationship between perceived control and the information disclosure behaviour. Accordingly, when the bootstrap values of the model are calculated, perceived risk and perceived benefit play a mediating role in the relationship between perceived control and information disclosure behaviour (0.234; 0.402).

The findings related to the hypotheses are presented in Table 6.

Table 5 Results of the correlation analysis conducted on the measurements using scales for privacy concerns, perceived control, risk, benefit, and personal health information disclosure

	Arithmetic Mean	Std. Deviation	1	2	3	4
1	3,01	0,98				
2	3,55	0,91	-0,19**			
3	3,98	1,53	0,71**	-0,17**		
4	5,49	1,22	-0,12**	0,44**	-0,08*	
5	4,93	1,50	-0,15**	0,37**	-0,13**	0,52**

** Correlation is significant at the 0.01 level (2-tailed). * Correlation is significant at the 0.05 level (2-tailed)

1 = Privacy Concern, 2 = Perceived Control, 3 = Perceived Risk, 4 = Perceived Benefit, 5 = Information Disclosure Behaviour)

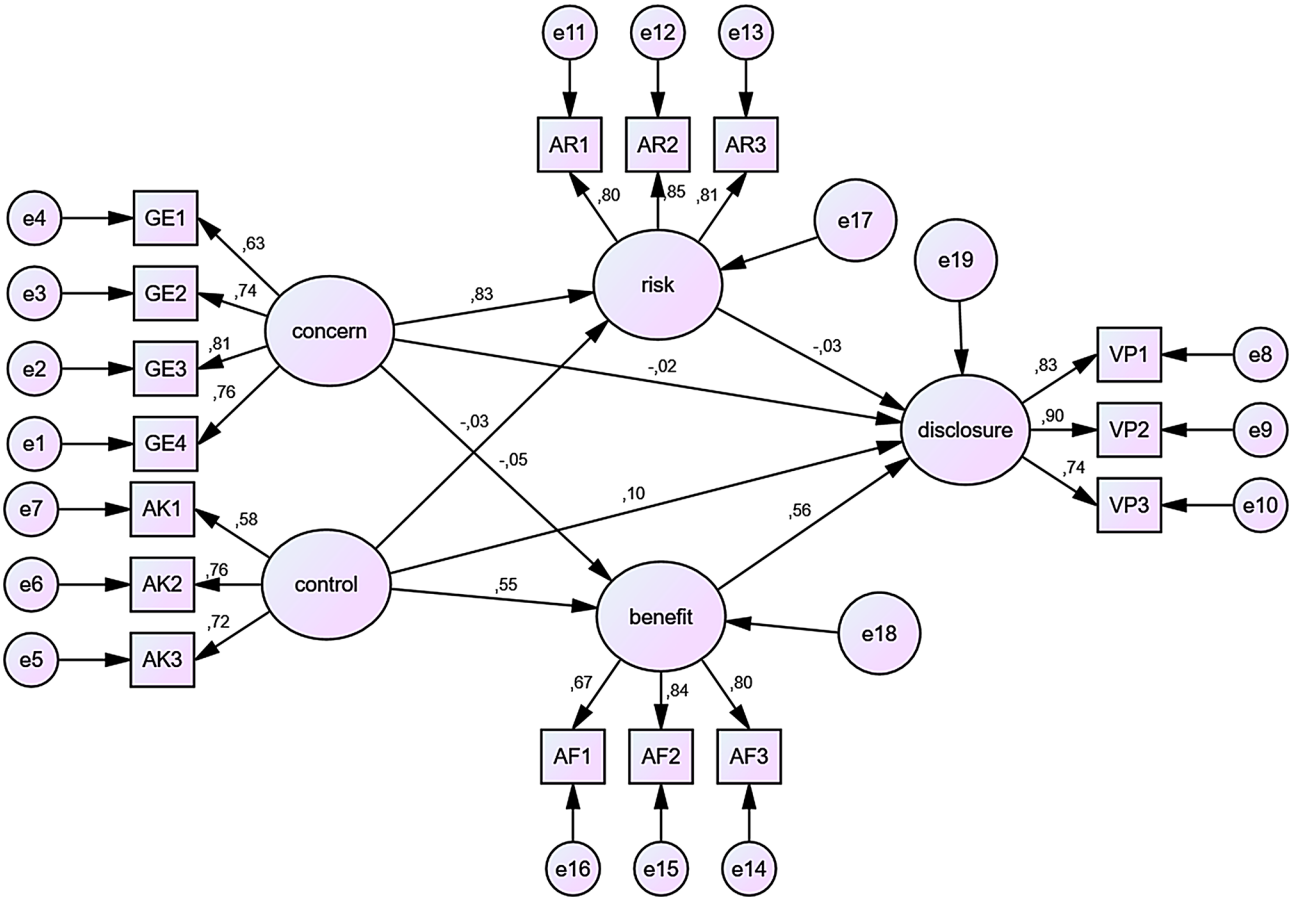

Fig. 3 The mediating role of perceived benefit and perceived risk in privacy concerns and personal health information disclosure

Table 6 Results for hypothesis testing in the study on privacy concerns, perceived control, risk, benefit, and personal health information disclosure

Hypothesis	β	*p*	Results
H1: Privacy concern is negatively related to the behaviour of information disclosure.	-0.03	0.041	Supported
H2: Perceived control is positively related to the behaviour of information disclosure.	0.73	0.000	Supported
H3: Perceived risk is positevly related to the privacy concern.	1.15	0.000	Supported
H4: Perceived risk mediates the relationship between privacy concern and information disclosure behaviour.	-0.02	0,521	Rejected
H5: Perceived risk mediates the relationship between perceived control and information disclosure behaviour.	0.10	0.000	Supported
H6: Perceived benefit is positively related to the perceived control.	0.73	0.000	Supported
H7: Perceived benefit mediates the relationship between privacy concern and behaviour of information disclosure.	-0.02	0,657	Rejected
H8: Perceived benefit mediates the relationship between perceived control and behaviour of information disclosure.	0.10	0.000	Supported

Discussion

This section is discussed under two headings: theoretical and practical implications.

Theoretical implications

According to the relevant literature, perceived benefit reduces privacy concerns and positively affects personal health data disclosure behaviour [59–61]. Research results also support this finding in the literature. Accordingly, perceived benefit and privacy concerns were negatively related, and information disclosure behaviour was positively related. Accordingly, there is a negative relationship between privacy concerns and information disclosure behaviour. As the privacy concerns of individuals increase in personal data disclosure, their information disclosure behaviour decreases. In this study, a positive relationship was found between perceived control and information disclosure behaviour [62]. Similarly, in his studies on perceived self-efficacy, Bandura addressed perceived control as an important determinant of health data disclosure behaviour and emphasized that the level of control had a positive effect on the information disclosure behaviour. Dhagarra et al. [29] aimed to measure the technology acceptance level of individuals in disclosure personal health data. Furthermore, in the same study, it was discovered that perceived benefit, perceived ease of use, trust, and privacy concerns were linked to the utilization of health technologies and the disclosure of information. In this context, it is essential to emphasize the importance of conducting and auditing processes in compliance with the General Data Protection Regulation (GDPR) to ensure respect for patient safety and privacy. Furthermore, the use of electronic health record systems should be secured with two-factor authentication encryption, and all procedures must be carried out with the patient's informed consent and explicit authorization.

According to Bansal et al. [4], perceived privacy risk in personal health data revolves around factors such as being in control of information, ensuring the security of information exchange, and ensuring that the entity collecting this information will adhere to established rules and regulations [4]. In this study, a negative relationship was found between perceived control and perceived risk, and a positive relationship was found between perceived control and perceived benefit. A significant relationship was found between individuals' privacy concerns and their perceived risk levels. Similarly, in a study conducted by Xu et al. [63] to examine the occurrence of privacy concerns of individuals in health services, a significant relationship was found between perceived risk and privacy concerns. In another study by Xu et al. [45], in healthcare services, a significant relationship was found between the risks individuals perceive in data sharing and privacy concerns. In this research, it was determined that perceived risk and perceived benefit did not have a mediating effect on the relationship between personal health data disclosure behaviour and privacy concerns. According to the relevant literature, perceived risks and benefits do not play a mediating role between privacy concerns and information disclosure behaviour, but information disclosure transparency plays a mediating role [64].

In this study, it was determined that perceived risk and perceived benefit play a mediating role in the relationship between information disclosure behavior and perceived control. According to the findings, perceived risks increase individuals' privacy concerns and decrease their intention to disclose personal health data. Conversely, perceived benefits reduce individuals' privacy concerns while increasing their intention to disclose personal health data. Therefore, enhancing perceived benefits and assuring individuals that disclosing personal health data will not pose any problems can facilitate data disclosure. A review of the literature reveals a lack of studies discussing these results. Consequently, this study appears to be both timely and capable of addressing this gap in the literature.

Practical implications

The findings of this study highlight crucial strategies for improving the management and practice of personal health data disclosure.

The necessity of these practices was also highlighted during the COVID-19 pandemic, a time when applications collecting and storing personal data became widespread. During the pandemic, many personal data, particularly personal health information, were collected through contact tracing applications. However, there were widespread public concerns regarding how these collected health data were stored and protected. Cioffi et al., [65] noted that personal data collected by contact tracing applications could be exploited by malicious third parties, which raised significant privacy concerns. Additionally, Bengio et al., [66] emphasized that privacy concerns arising from contact tracing applications could be mitigated through informed consent and transparency. Therefore, it can be suggested that privacy concerns and perceived risks, which pose barriers to the effective use of collected personal health data, can be alleviated through measures such as the principle of transparency and informed consent.

The research indicates that perceived risks are inversely related to the intention to disclose personal health data. To address this, health technology providers should focus on implementing measures that effectively mitigate privacy concerns. This can be achieved through robust data protection policies, security certifications, and transparent communication about data handling practices. By

ensuring that users feel their data is secure and well-protected, providers can reduce perceived risks and encourage greater willingness to disclose health information. Conversely, the study also reveals that perceived benefits positively influence the intention to disclose personal health data. To capitalize on this, health service providers should emphasize the tangible advantages of data sharing, such as enhanced health services, personalized treatment plans, and early diagnosis opportunities. Informational campaigns and educational programs that clearly articulate these benefits can improve user attitudes towards data sharing. Additionally, enhancing user education about data protection mechanisms and ensuring high levels of transparency can build trust and alleviate privacy concerns. These strategies collectively offer a comprehensive approach to facilitating more effective and widespread health data disclosure.

Conclusion

This study underscores the sensitive and critical nature of the issue by highlighting the mediating role of perceived risk and perceived benefit in the relationship between health information disclosure behaviour, privacy concerns, and perceived control. A literature review revealed that the dimensions addressed on the subject are evaluated separately in different sectors, but these dimensions in the field of health have not been examined together in any study. Therefore, based on results obtained in this research, it is thought that this study will contribute to the field. On the other hand, within the scope of the research, in the relationship between privacy concerns and information disclosure behaviour, since it has been determined that perceived risks and benefits have a mediating role, it is recommended that other researchers investigate whether other variables have a mediating role.

As a result, to address the issues investigated in the study and minimize concerns, training sessions for scientists, politicians, companies involved in health information technology production, and healthcare institutions and organizations are recommended. This will help raise societal awareness and foster a sense of security. In essence, considering that personal health data are a concept that has recently gained recognition for its significance, it is imperative to educate healthcare personnel on safeguarding patient data privacy. Hospital administrators and administrative units bear significant responsibility in this regard. Therefore, organizing data privacy seminars for all healthcare personnel can effectively enhance awareness among employees.

Limitations

This research has several limitations. First, the use of quantitative methods restricts the ability to conduct an in-depth analysis. Second, the study is limited to the 635 participants who agreed to participate and complete the surveys. Additionally, the research is constrained by the specific time period during which it was conducted. Despite these limitations, this study contributes to the field by providing a reliable and generalizable perspective on personal health data disclosure. For more comprehensive findings, future research could employ different research methods and include diverse populations or samples.

Abbreviations

APCO	Antecedents Antecedents, Privacy, Concerns, Outcomes
CFA	Confirmatory Factor Analysis
SEM	Structural Equation Modeling

Acknowledgements

Not applicable.

Author contributions

HNA: study conception, research design, interpretation, analysis, and drafting of the manuscript. ŞY: Interpretation, analysis, drafting of the manuscript draft, and research coordination. All authors contributed to the analysis, writing, and critical review of the manuscript and approved the final version for submission.

Funding

Not applicable.

Data availability

The datasets used and/or analysed as part of the current study are available from the corresponding author upon reasonable request.

Declarations

Ethics approval and consent to participate

This study was carried out with the approval of the Ethics Committee of Selcuk University, aged 25/05/2022 and numbered 2022/05. A signed subject consent form in accordance with the Declaration of Helsinki was obtained from each participant. Informed consent was obtained from all participants in the study online. The principles of the Declaration of Helsinki were followed in the collection of research data and in all processes associated with this research.

Consent for publication

Not applicable.

Competing interests

The authors declare no competing interests.

Received: 6 June 2024 / Accepted: 3 October 2024
Published online: 11 October 2024

References

1. Chaudhry A, Crowcroft J, Howard H, Madhavapeddy A, Mortier R, Haddadi H et al. Personal data: thinking inside the box. 2015 [cited 2023 Oct 26]; https://www.repository.cam.ac.uk/handle/1810/248792
2. Li J. Ensuring privacy in a personal health record system. Computer. 2015;48(2):24–31.
3. Youn S. Determinants of online privacy concern and its influence on privacy Protection behaviors among Young adolescents. J Consum Aff. 2009;43(3):389–418.
4. Bansal G, Zahedi FM, Gefen D. The impact of personal dispositions on information sensitivity, privacy concern and trust in disclosing health information online. Decis Support Syst. 2010;49(2):138–50.
5. Mehraeen E, Ayatollahi H, Ahmadi M. Health information security in hospitals: the application of security safeguards. Acta Informatica Med. 2016;24(1):47.

6. Xu H, Luo X (Robert), Carroll JM, Rosson MB, editors. The personalization privacy paradox: An exploratory study of decision making process for location-aware marketing. Decision Support Systems. 2011;51(1):42–52.
7. Princi E, Krämer NC. Out of control–privacy calculus and the effect of perceived control and moral considerations on the usage of IoT healthcare devices. Front Psychol. 2020;11:1–15.
8. Infurna FJ, Gerstorf D, Zarit SH. Examining dynamic links between perceived control and health: longitudinal evidence for differential effects in midlife and old age. Dev Psychol. 2011;47(1):9–18.
9. Alonso-Ferres M, Imami L, Slatcher RB. Untangling the effects of partner responsiveness on health and well-being: the role of perceived control. J Social Personal Relationships. 2020;37(4):1150–71.
10. Sun Y, Wang N, Shen XL, Zhang JX. Location information disclosure in location-based social network services: privacy calculus, benefit structure, and gender differences. Comput Hum Behav. 2015;52:278–92.
11. George R, D'Alessandro S, Mehmet MI, Nikidehaghani M, Evans MM, Laud G, et al. On the path to Decolonizing Health Care Services: the role of marketing. J Mark. 2024;88(1):138–59.
12. Choi J, Lee A, Ok C. The effects of consumers' perceived risk and benefit on attitude and behavioral intention: a study of Street Food. J Travel Tourism Mark. 2013;30(3):222–37.
13. Dinev T, Xu H, Smith JH, Hart P. Information privacy and correlates: an empirical attempt to bridge and distinguish privacy-related concepts. Eur J Inform Syst. 2013;22(3):295–316.
14. Smith HJ, Dinev T, Xu H. Information privacy research: an interdisciplinary review. MIS Q. 2011;989–1015.
15. Buck C, Dinev T, Anaraky RG, Revisiting APCO. In: Knijnenburg BP, Page X, Wisniewski P, Lipford HR, Proferes N, Romano J, editors. Modern Socio-Technical Perspectives on Privacy [Internet]. Cham: Springer International Publishing; 2022 [cited 2023 Dec 24]. pp. 43–60. https://doi.org/10.1007/978-3-030-82786-1_3
16. Dinev T, McConnell AR, Smith HJ. Research Commentary: informing privacy research through Information systems, psychology, and behavioral economics: thinking outside the 'APCO' Box. Inform Syst Res. 2015;26(4):639–55.
17. Acquisti A, Grossklags J. Privacy and rationality in individual decision making. IEEE Secur Priv. 2005;3(1):26–33.
18. Buchanan T, Paine C, Joinson AN, Reips U. Development of measures of online privacy concern and protection for use on the internet. J Am Soc Inf Sci. 2007;58(2):157–65.
19. Malhotra NK, Kim SS, Agarwal J. Internet users' information privacy concerns (IUIPC): the Construct, the Scale, and a causal model. Inform Syst Res. 2004;15(4):336–55.
20. Smith HJ, Milberg SJ, Burke SJ. Information privacy: measuring individuals' concerns about organizational practices. MIS Q. 1996;20(2):167–96.
21. Yao MZ, Rice RE, Wallis K. Predicting user concerns about online privacy. J Am Soc Inf Sci. 2007;58(5):710–22.
22. Chen R. Living a private life in public social networks: an exploration of member self-disclosure. Decis Support Syst. 2013;55(3):661–8.
23. Nemec Zlatolas L, Welzer T, Hölbl M, Heričko M, Kamišalić A. A model of perception of privacy, trust, and self-disclosure on online social networks. Entropy. 2019;21(8):772.
24. Culnan MJ, Armstrong PK. Information privacy concerns, Procedural Fairness, and Impersonal Trust: an empirical investigation. Organ Sci. 1999;10(1):104–15.
25. Lee N, Kwon O. A privacy-aware feature selection method for solving the personalization–privacy paradox in mobile wellness healthcare services. Expert Syst Appl. 2015;42(5):2764–71.
26. Milne GR, Pettinico G, Hajjat FM, Markos E. Information sensitivity typology: mapping the degree and type of risk consumers perceive in Personal Data sharing. J Consum Aff. 2017;51(1):133–61.
27. Li H, Sarathy R, Xu H. The role of affect and cognition on online consumers' decision to disclose personal information to unfamiliar online vendors. Decis Support Syst. 2011;51(3):434–45.
28. Borena B, Belanger F, Ejigu D. Social Networks and Information Privacy: A Model for Low-income Countries. In Chicago: Citeseer; 2013 [cited 2023 Oct 26]. pp. 1–9. https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=8bb38cf4c8fc5b189008f2e16892d6a665694ae7
29. Dhagarra D, Goswami M, Kumar G. Impact of trust and privacy concerns on technology acceptance in healthcare: an Indian perspective. Int J Med Informatics. 2020;141:104164.
30. George J, Bhila T. Security, confidentiality and privacy in health of healthcare data. Intern J Trend Sci Res Dev. 2019;4:373–7.
31. Wang T, Duong TD, Chen CC. Intention to disclose personal information via mobile applications: a privacy calculus perspective. Int J Inf Manag. 2016;36(4):531–42.
32. Hofmann W, Luhmann M, Fisher RR, Vohs KD, Baumeister RF. Yes, but are they happy? Effects of Trait Self-Control on Affective Well-being and life satisfaction. J Pers. 2014;82(4):265–77.
33. Robinson SA, Lachman ME. Perceived control and aging: a mini-review and directions for future research. Gerontology. 2017;63(5):435–42.
34. Beck EJ, Gill W, De Lay PR. Protecting the confidentiality and security of personal health information in low- and middle-income countries in the era of SDGs and Big Data. Global Health Action. 2016;9(1):1–7.
35. Hong IB. Understanding the consumer's online merchant selection process: the roles of product involvement, perceived risk, and trust expectation. Int J Inf Manag. 2015;35(3):322–36.
36. Win KT. A Review of Security of Electronic Health Records. Health Inform Manage. 2005;34(1):13–8.
37. Das TK, Teng BS. Between Trust and Control: developing confidence in Partner Cooperation in Alliances. Acad Manage Rev. 1998;23(3):491.
38. Krasnova H, Spiekermann S, Koroleva K, Hildebrand T. Online Social networks: why we disclose. J Inform Technol. 2010;25(2):109–25.
39. Hajli N, Lin X. Exploring the security of information sharing on social networking sites: the role of perceived control of information. J Bus Ethics. 2016;133:111–23.
40. Forsythe SM, Shi B. Consumer patronage and risk perceptions in internet shopping. J Bus Res. 2003;56(11):867–75.
41. Boshoff C, Schlechter C, Ward SJ. Consumers' perceived risks associated with purchasing on a branded web site: the mediating effect of brand knowledge. South Afr J Bus Manage. 2011;42(1):45–54.
42. Becker M. Understanding users' health information privacy concerns for health wearables. In 2018 [cited 2023 Oct 26]. pp. 3261–70. https://aisel.aisnet.org/hicss-51/hc/security_for_healthcare/2/
43. Thilakanathan D, Calvo RA, Chen S, Nepal S, Glozier N. Facilitating Secure Sharing of Personal Health Data in the Cloud. JMIR Med Inf. 2016;4(2):e15.
44. Tanadi T, Samadi B, Gharleghi B. The impact of Perceived risks and Perceived benefits to improve an online intention among Generation-Y in Malaysia. ASS. 2015;11(26):226–38.
45. Xu H, Dinev T, Smith J, Hart P. Information privacy concerns: linking individual perceptions with institutional privacy assurances. J Association Inform Syst. 2011;12(12):1.
46. Park M, Chai S. The value of Personal Information: an exploratory study for types of Personal Information and its value. APJIS. 2018;28(3):154–66.
47. Berndt AE. Sampling methods. J Hum Lact. 2020;36(2):224–6.
48. Coşkun R, Altunışık R, Yıldırım E. Sosyal Bilimlerde Araştırma Yöntemleri SPSS Uygulamaları. 8. baskı. Sakarya Yayıncılık; 2015. 398 p.
49. Etikan I, Bala K. Sampling and sampling methods. Biometrics Biostatistics Int J. 2017;5(6):00149.
50. Gürbüz S, Şahin F. Sosyal Bilimlerde Araştırma Yöntemleri [İnternet]. 3. baskı. Ankara: Seçkin Yayıncılık; 2018 [cited 2024 Mar 19]. https://www.seckin.com.tr/kitap/733449175
51. Sun Y, Fang S, Hwang Y. Investigating privacy and information disclosure behavior in social electronic commerce. Sustainability. 2019;11(12):3311.
52. Li H, Luo XR, Zhang J, Xu H. Resolving the privacy paradox: toward a cognitive appraisal and emotion approach to online privacy behaviors. Inf Manag. 2017;54(8):1012–22.
53. Hair J, Black W, Babin B, Anderson R. Multivariate Data Analysis: Pearson New International Edition. Harlow; 2013.
54. Bagozzi RP. Evaluating Structural equation models with unobservable variables and measurement error: a comment. J Mark Res. 1981;18(3):375–81.
55. Hooper D, Coughlan J, Mullen M. Evaluating model fit: a synthesis of the structural equation modelling literature. In: 7th European Conference on research methodology for business and management studies [Internet]. 2008 [cited 2023 Oct 26]. pp. 195–200. https://books.google.com/books?hl=tr&lr=&id=ZZoHBAAAQBAJ&oi=fnd&pg=PA195&dq=Evaluating+model+fit:+a+synthesis+of+the+structural+equation+modelling+literature&ots=gW3T_qXt97&sig=B9lojmfo6Wl0TCjr-VEjWMkZgLQ
56. Li S, Rao SS, Ragu-Nathan TS, Ragu-Nathan B. Development and validation of a measurement instrument for studying supply chain management practices. J Oper Manag. 2005;23(6):618–41.
57. Steiger JH. Understanding the limitations of global fit assessment in structural equation modeling. Pers Indiv Differ. 2007;42(5):893–8.
58. Bentler PM. Comparative fit indexes in structural models. Psychol Bull. 1990;107(2):238.

59. Cocosila M, Archer N. Perceptions of chronically ill and healthy consumers about electronic personal health records: a comparative empirical investigation. BMJ open. 2014;4(7):e005304.
60. Emani S, Yamin CK, Peters E, Karson AS, Lipsitz SR, Wald JS, et al. Patient perceptions of a personal health record: a test of the diffusion of innovation model. J Med Internet Res. 2012;14(6):e2278.
61. Park J, Snell W, Ha S, Chung TL. Consumers' post-adoption of M-services: Interestin Future M-services based on ConsumerEvaluations of current M-services. J Electron Commer Res. 2011;12(3):165–75.
62. Bandura A. Self-efficacy: toward a unifying theory of behavioral change. Psychol Rev. 1977;84(2):191–215.
63. Xu H, Dinev T, Smith HJ, Hart P. Examining the formation of individual's privacy concerns: Toward an integrative view. ICIS 2008 Proceedings. 2008;1–16.
64. Awad NF, Krishnan MS. The personalization privacy paradox: an empirical evaluation of information transparency and the willingness to be profiled online for personalization. MIS Q. 2006;30(1):13–28.
65. Cioffi A, Lugi C, Cecannecchia C. Apps for COVID-19 contact-tracing: too many questions and few answers. Ethics Med Public Health. 2020;15:100575.
66. Bengio Y, Ippolito D, Janda R, Jarvie M, Prud'homme B, Rousseau JF, et al. Inherent privacy limitations of decentralized contact tracing apps. J Am Med Inf Assoc. 2021;28(1):193–5.

Publisher's note