A Study on Patients' Privacy in AI Medical Applications from the Perspective of Privacy Calculus

Yijia Qiu Xiaowen Xu

School of Humanities,University of Chinese Academy of Sciences,Beijing,100049

Abstract: **[Purpose]** This study investigates the mechanism through which users' perception of intelligent medical platforms in AI medical applications influences their privacy concerns and disclosure intentions,mediated by perceived benefits and risks. The findings aim to provide strategic recommendations for privacy regulation and user profiling in the context of smart healthcare. **[Method]** Drawing upon Privacy Calculus Theory, this research constructs a theoretical path: "Usage Perception(Perceived Ease of Use,Perceived Usefulness, Perceived Reliability, Perceived Transparency) → Perceived Benefits/Perceived Risks → Privacy Concern." Using a sample of users with experience in AI medical applications, 568 valid data points were collected via surveys. Reliability and validity tests,along with Structural Equation Modeling (SEM) ,were conducted using SPSS 26.0 and AMOS 24.0 to verify the hypotheses. **[Results/Conclusion]** The results indicate that Perceived Ease of Use and Perceived Usefulness significantly and positively impact Perceived Benefits while negatively impacting Perceived Risks. Perceived Reliability and Perceived Transparency significantly reduce Perceived Risks but do not have a significant positive effect on Perceived Benefits. Furthermore, Perceived Benefits negatively influence Privacy Concern, whereas Perceived Risks exert a positive influence. Notably, Privacy Concern positively affects Privacy Disclosure Intention, illustrating the "Privacy Paradox" in medical contexts. This study theoretically extends the boundaries of the Privacy Calculus model in healthcare and enriches the dimensions of the Technology Acceptance Model (TAM) in privacy research, revealing the internal logic of the privacy paradox in intelligent medical scenarios.

Keywords:AI Medical Applications;Privacy Calculus Theory;Technology Acceptance Model(TAM);Privacy Disclosure Intention

Introduction

In today's information-oriented society, Artificial Intelligence (AI) has been extensively integrated into human production and daily life, marking a new stage of Human-AI Interaction (HAII) characterized by intelligence, personalization, and bidirectional engagement (Jiang et al., 2022). Chatbots are AI-powered applications that simulate interactive human conversations using pre-calculated key user phrases and auditory or text-based signals. The introduction of Large Language Models (LLMs) has further enhanced the conversational capabilities of chatbots, enabling them to navigate more complex and diverse dialogue scenarios (Wu et al., 2023). These technological breakthroughs allow for more personalized and dynamic interactions, improving user experience and assuming an increasingly vital role in the medical field. AI is profoundly reshaping the delivery of healthcare services globally, driving transformative changes in inclusive healthcare, technical cooperation, industrial upgrading, and public health prevention.

As the medical sector integrates deeply with AI, intelligent medical technology—driven by "data & algorithms"—is advancing rapidly (Zhou et al., 2024). The application scenarios for chatbots in healthcare have expanded from early health Q&A to various domains such as disease screening, chronic disease management, psychological support, medical education, and clinical training. These applications not only significantly improve the efficiency of medical services but also provide patients with a more convenient medical experience, serving as a robust technical support for the healthcare system (Bao et al., 2023; Thirunavukarasu et al., 2023). In this process, the AI system is no longer a transparent tool; through algorithms, interfaces, and prompts, it actively or passively participates in the dissemination, collection, and processing of patient information, with its internal logic influencing patients' privacy decisions. However, chatbots face severe privacy and security risks when processing user data. Despite the maturation of data encryption and anonymization technologies, the possibility of privacy breaches persists, which in turn affects patients' perceptions of system reliability and their intention to disclose personal information (Khalid et al., 2023). Given the sensitivity of medical data, it is imperative for stakeholders to continuously update existing data management practices and develop new methods that facilitate AI research while protecting

data privacy.

In recent years, academic research on privacy disclosure intention and behavior has primarily focused on social networking, e-commerce, and healthcare (Zhu et al., 2022); however, few studies have considered the impact of specific systemic features of medical chatbots on subjective perception and privacy concerns (Chen & Cliquet, 2020). Relevant research indicates that addressing technical and legal perspectives can simultaneously reduce user privacy concerns and encourage the disclosure of personal information. Regarding theoretical development, the Privacy Calculus model employs a risk-reward trade-off perspective to describe individuals' self-disclosure intentions regarding their information. Researchers have used this as a theoretical foundation, either by introducing additional variables or combining it with multiple theories to construct comprehensive theoretical frameworks. This study first introduces the Technology Acceptance Model (TAM) and Perceived Risk Theory to construct a conceptual path: "Usage Perception (Perceived Ease of Use, Perceived Usefulness, Perceived Reliability, Perceived Transparency) → Perceived Benefits/Perceived Risks → Privacy Concern." It systematically analyzes how users' perceptions of intelligent medical platforms are mediated by benefits and risks to ultimately influence their level of privacy concern. Theoretically, this paper enriches the body of research on privacy behavior and provides a more comprehensive revelation of the underlying mechanisms between privacy concern, disclosure intention, and actual disclosure behavior from the user's perspective. Practically, it offers strategic recommendations for privacy regulation and user profiling analysis within intelligent medical contexts.

Methodology

This paper combines the Technology Acceptance Model (TAM), which explains how users accept and use technology, with two key variables: perceived reliability and perceived transparency. Perceived reliability is users' belief that the chatbot performs consistently as expected. Perceived transparency is users' perception of the chatbot's openness in communicating its processes. The study explores how technical characteristics of medical chatbots—automated systems providing medical information or guidance—influence privacy concerns. It then examines users' willingness to disclose private in

formation. The analysis uses the concept of privacy computing, which includes methods and technologies designed to protect users' data privacy during computational processes, such as secure multi-party computation and differential privacy.

1.1 Perceived Ease of Use and Perceived Usefulness

According to the Technology Acceptance Model, users are more likely to recognize a technology's value if it is easy to use (Davis, 1989; Venkatesh & Davis, 2000). In the context of medical chatbot consultations, user-friendly systems reduce learning obstacles and cognitive load, delivering benefits like efficiency and improved diagnostics. Empirical research confirms this link between ease of use and favorable value assessments (Holden & Karsh, 2010). Likewise, perceived usefulness plays a decisive role in technology acceptance. For example, patients identify AI diagnostics as beneficial if they improve treatment quality and efficiency, which can yield advantages such as enhanced diagnostic accuracy and personalized care plans (Palos-Sánchez et al., 2021). Conversely, complex systems may foster uncertainty and risk (Slovic, 1987). Further studies show that perceptions of ease of use influence risk assessments (Featherman & Pavlou, 2003). When users struggle with a system, they may doubt its privacy protections, elevating risk perceptions. Based on this progression, these hypotheses are proposed:

H1a: Perceived ease of use positively influences perceived benefits.

H1b: Perceived ease of use negatively influences perceived risks.

H2a: Perceived usefulness positively influences perceived benefits.

H2b: Perceived usefulness negatively influences perceived risks.

1.2 Perceived Transparency and Perceived Reliability

Expanding on this, increasing transparency in data processing emerges as an effective strategy to enhance perceived benefits. Research indicates that clear information disclosure can build users' trust in technology and increase perceived value (Schnackenberg & Tomlinson, 2016). When AI healthcare systems provide detailed explanations about data usage, safeguards, and decision processes, patients better understand the medical benefits of sharing information, such as personalized services and improved treatment plans (Esmaeilzadeh, 2019). Furthermore, clarity about privacy policies and security measures enables users to form positive judgments about data sharing. Such transpare

ncy regarding data collection and processing can reduce uncertainty and anxiety. Accor dingly, this paper proposes the following hypotheses:

H3a: Perceived reliability positively influences perceived benefits.

H3b: Perceived reliability negatively influences perceived risks.

H4a: Perceived transparency positively influences perceived benefits.

H4b: Perceived transparency negatively influences perceived risks.

1.3 Perceived Benefits and Perceived Risks

Continuing with privacy calculus theory, users weigh perceived benefits against pe rceived risks when making privacy decisions (Dinev & Hart, 2006). High perceived be nefits can reduce privacy concerns; in AI healthcare, strong expected benefits often di minish worries over data breaches. Existing research also shows that risk sensitivity a mplifies privacy concerns (Malhotra, Kim, & Agarwal, 2004). When health data is hig hly sensitive, perceived risk increases concern for privacy. As a result, this paper prop oses the following hypotheses:

H5: Perceived benefits negatively influence privacy concerns.

H6: Perceived risks positively influence privacy concerns.

1.4 Privacy Concerns

Privacy concerns cover a person's anticipation of privacy loss, encompassing infor mation collection, unauthorized access, data inaccuracies, and secondary use (Smith et al., 1996). While higher privacy concerns typically reduce willingness to disclose infor mation, some studies argue that users balance perceived benefits with risks. This prom pts the privacy paradox—a gap between concern and actual disclosure (Zhu Guang, 20 22). For example, in intelligent healthcare, individuals may share data despite substanti al privacy concerns to achieve more customized or precise care. Building on these insi ghts, the following hypothesis is proposed:

H7: Privacy concerns positively influence willingness to disclose privacy.

Based on the above hypotheses and analysis, the model constructed in this paper is illustrated in Figure 1.

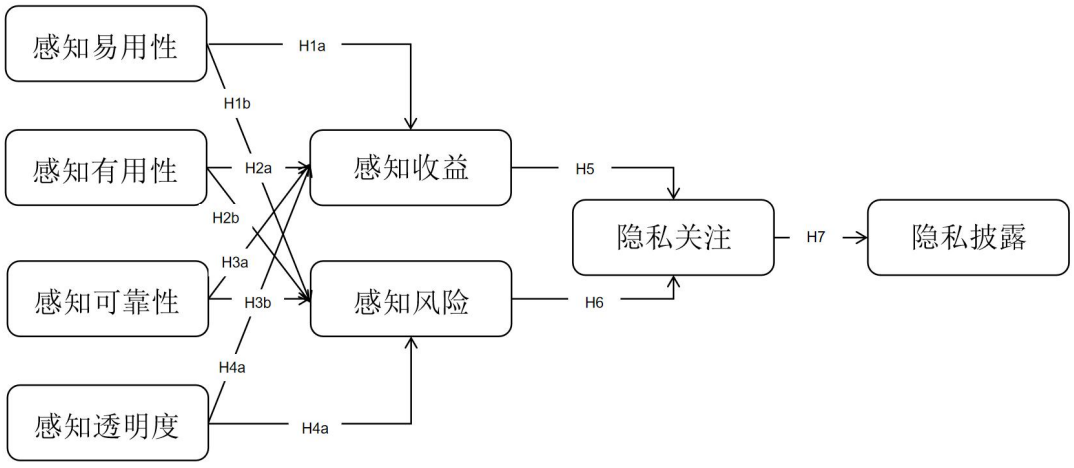

Fig 1 Research Model

2.1 Questionnaire Design

This study focuses on users of intelligent chatbots based on medical large language models, which are AI systems trained on substantial amounts of medical data to interpret and generate human language. Specifically, the study surveyed individuals aged 16 and above who have previously used such medical chatbots. The survey consists of three sections: a definition of the intelligent healthcare platform and clarification of the questionnaire's objectives; collection of demographic statistics; and a thematic questionnaire forming the measurement scale. The measurement scale includes eight latent variables (unobserved factors inferred from observed data) and thirty-two observed variables (directly measured questionnaire items). All questionnaire items use a five-point Likert scale: 1 = "Strongly Disagree," 2 = "Somewhat Disagree," 3 = "Neutral (Undecided)," 4 = "Somewhat Agree," and 5 = "Strongly Agree." All scale items are sourced from both domestic and international literature and revised to suit the study's requirements, see attachment for details.

2.2 Data Collection

A snowball sampling method was employed to select 49 respondents with experience using smart medical health platforms as pre-test subjects, identifying potential issues in questionnaire wording and semantics. Reliability and validity tests were conducted on the questionnaire, revealing Cronbach's Alpha values exceeding 0.6 for all variabl

es and Average Variable Extraction (AVE) values surpassing 0.5. These results indicate the questionnaire possesses high levels of reliability and validity. The formal questionnaire was distributed to users who had utilized smart medical health platforms. Distribution was conducted via the professional domestic survey platform ”Credamo Jianshu” (https://www.credamo.com/home.html#/). To ensure high survey quality, 400 paid questionnaires were distributed through this platform. Additionally, 200 questionnaires were distributed via social media platforms Xiaohongshu and Douban communities to ensure broad representation of the survey population. Ultimately, 600 questionnaires were distributed for this study. After excluding 32 non-compliant responses, 568 valid questionnaires were obtained. After analyzing detailed descriptive statistics of respondents, comparison of the age distribution revealed alignment with that of generative AI users published in the China Internet Network Information Center's “Generative Artificial Intelligence Application Development Report (2024).” Thus, no significant sampling bias was identified. Sample distribution characteristics are shown in Table 1.

Table 1 Sample Distribution Characteristics（N=568）

Project	**Variable**	**Frequency**	**Percentage（%）**	**Effective percentage（%）**	**Cumulative percentage（%）**
Gender	Male	368	64.8	64.8	64.8
	Female	200	35.2	35.2	100.0
Academic qualifications	Specialist	94	16.5	16.5	16.5
	Undergraduate	129	22.7	22.7	39.3
	Master's degree	257	45.2	45.2	84.5
	Doctor	88	15.5	15.5	100.0
Age	0-20 years old	45	7.9	7.9	7.9
	21-30 years old	443	78.0	78.0	85.9
	31-40 years old	55	9.7	9.7	95.6
	41-50 years old	15	2.6	2.6	98.2
	51-60 years old	10	1.8	1.8	100.0
Income	Under10,000	174	30.6	30.6	30.6
	10,000-50,000	133	23.4	23.4	54.0
	50,000-100,000	101	17.8	17.8	71.8
	100,000-150,000	65	11.4	11.4	83.3
	150,000-200,000	47	8.3	8.3	91.5
	200,000-300,000	30	5.3	5.3	96.8
	Over 300,000	18	3.2	3.2	100.0
Marital status	Married	110	19.4	19.4	19.4

Project	Variable	Frequency	Percentage（%）	Effective percentage （%）	Cumulative percentage （%）
	Unmarried	458	80.6	80.6	100.0

2.3 Model Analysis and Data Results

This study primarily employed SPSS 26.0 and AMOS 24.0 software to test the proposed model. The data analysis process comprised two main components: evaluating the measurement model through reliability and validity assessments, and verifying hypotheses regarding the structural model.

2.3.1 Reliability Testing

The overall Cronbach's α for the 32 measurement items in the questionnaire was 0.850, exceeding the minimum reliability threshold of 0.600. This indicates good reliability for all variables in this study. The corrected item total correlation (CITC) values for each item exceeded 0.600. After item deletion, the Cronbach’s α values remained above the minimum reliability threshold of 0.700, indicating relatively high reliability for the scales used in this study.

Table 2 Reliability Testing

Variable	Title	CITC	Cronbach's α value after item deletion	Cronbach's α value
Perceived usability	PEOU1	0.736	0.828	0.870
	PEOU2	0.705	0.840	
	PEOU3	0.720	0.835	
	PEOU4	0.730	0.831	
Perceived usefulness	PU1	0.693	0.786	0.838
	PU2	0.660	0.800	
	PU3	0.678	0.793	
	PU4	0.656	0.803	
Perceived reliability	PREL1	0.746	0.808	0.862
	PREL2	0.711	0.822	
	PREL3	0.692	0.830	
	PREL4	0.690	0.833	
Perceived transparency	PT1	0.802	0.833	0.885
	PT2	0.775	0.842	
	PT3	0.727	0.861	
	PT4	0.699	0.873	
Perceived benefits	PB1	0.738	0.782	0.846
	PB2	0.698	0.799	
	PB3	0.660	0.815	
	PB4	0.642	0.824	
Perceiving risk	PR1	0.678	0.827	0.857
	PR2	0.666	0.835	
	PR3	0.740	0.802	
	PR4	0.727	0.806	
Privacy concerns	PC1	0.770	0.812	0.868
	PC2	0.738	0.825	
	PC3	0.705	0.838	
	PC4	0.677	0.853	
Privacy disclosure consent	PDI1	0.740	0.836	0.875
	PDI2	0.715	0.846	
	PDI3	0.729	0.841	
	PDI4	0.742	0.835	
Total	32	/	/	0.850

2.3.2 Validity Testing

Validity reflects the degree to which measurement results are meaningful. This stu

dy employed both convergent validity and discriminant validity to assess data validity. Generally, convergent validity is considered adequate when factor loadings exceed 0.7 and the average extracted variance (AVE) exceeds 0.5. Statistical results indicate that the scales in this study demonstrate good convergent validity (see Table 3). The crite rion for discriminant validity is typically that the square root of the average extracted variance for each latent variable exceeds its correlation coefficient with other latent va riables. Measurement results show significant differences among the latent variables in this study, indicating good discriminant validity (see Table 4).

Table 3 Convergent Validity Test

Variable	**Measurement item**	**Standard load factor**	**S.E.**	**C.R.**	**p**	**CR**	**AVE**
Perceived usability	PEOU1	0.803				0.870	0.627
	PEOU2	0.778	0.052	19.316	***		
	PEOU3	0.787	0.048	19.576	***		
	PEOU4	0.799	0.054	19.890	***		
Perceived usefulness	PU1	0.777				0.840	0.567
	PU2	0.732	0.058	16.698	***		
	PU3	0.765	0.054	17.411	***		
	PU4	0.738	0.060	16.842	***		
Perceived reliability	PREL1	0.833				0.863	0.612
	PREL2	0.775	0.048	19.779	***		
	PREL3	0.769	0.046	19.612	***		
	PREL4	0.750	0.052	19.013	***		
Perceived transparency	PT1	0.875				0.888	0.664
	PT2	0.836	0.041	24.214	***		
	PT3	0.794	0.040	22.515	***		
	PT4	0.750	0.045	20.685	***		
Perceived benefits	PB1	0.824				0.849	0.585
	PB2	0.776	0.051	19.098	***		
	PB3	0.745	0.049	18.276	***		
	PB4	0.710	0.054	17.305	***		
Perceiving risk	PR1	0.758				0.860	0.605
	PR2	0.732	0.066	16.895	***		
	PR3	0.826	0.058	18.978	***		
	PR4	0.793	0.060	18.313	***		
Privacy concerns	PC1	0.851				0.872	0.630
	PC2	0.803	0.045	21.418	***		
	PC3	0.780	0.043	20.664	***		
	PC4	0.737	0.051	19.201	***		
Privacy disclosure consent	PDI1	0.806				0.875	0.637

Variable	Measurement item	Standard load factor	S.E.	C.R.	p	CR	AVE
	PDI2	0.777	0.052	19.620	***		
	PDI3	0.798	0.047	20.240	***		
	PDI4	0.811	0.053	20.628	***		

Table 4 Discriminant Validity Test

变量	1	2	3	4	5	6	7	8
Perceived usability	0.792							
Perceived usefulness	0.353	0.753						
Perceived reliability	0.355	0.332	0.782					
Perceived transparency	0.254	0.184	0.326	0.815				
Perceived benefits	0.412	0.337	0.274	0.201	0.765			
Perceiving risk	0.371	0.309	0.381	0.266	0.306	0.778		
Privacy concerns	0.348	0.329	0.365	0.198	0.312	0.341	0.794	
Privacy disclosure consent	0.345	0.442	0.427	0.265	0.482	0.370	0.328	0.798

2.3.3 Model Hypothesis Testing

This study employed AMOS 24.0 software to test the structural equation model. The model fit was assessed based on the fit indices provided by AMOS, with results presented in Table 5. The study employed multiple fit indices: the chi-square-to-degrees-of-freedom ratio (χ^2/df), root mean square error of approximation (RMSEA), goodness-of-fit index (GFI), adjusted goodness-of-fit index (AGFI), comparative fit index (CFI), normality fit index (NFI), and inflection fit index (IFI). As shown in the Table 5, all fit indices fall within recommended ranges, indicating that the research model exhibits satisfactory fit.

Table 5 Structural Equation Model Fit Test Results

Common indicators	x 2/df	GFI	AGFI	NFI	IFI	TLI	CFI	RMSEA
Statistical value	1.731	0.924	0.910	0.920	0.965	0.961	0.965	0.036
Reference value	<3	>0.8	>0.8	>0.9	>0.9	>0.9	>0.9	<0.08
Compliance status	Compliance	Compliance	Compliance	Compliance	Compliance	Compliance	Compliance	Compliance

This study proposes seven sets comprising 11 hypotheses. The path coefficients, hypothesis test conclusions, and corresponding significance levels are presented in Figure 2. Perceived ease of use exerts a significant positive influence on perceived benefits ($\beta = 0.304$, $P < 0.001$) and a significant negative influence on perceived risks ($\beta = -0.221$, $P < 0.001$), supporting both H1a and H1b. Perceived usefulness positively influenced perceived benefits ($\beta = 0.198$, $P < 0.001$) and negatively influenced perceived risks ($\beta = -0.145$, $P = 0.004$), supporting H2a and H2b. The positive effect of perceived reliability on perceived benefits was not significant ($\beta = 0.092$, $P = 0.077$), failing to support H3a; however, its negative effect on perceived risk was significant ($\beta = -0.229$, $P < 0.001$), supporting H3b. Perceived transparency had no significant effect on perceived benefits ($\beta = 0.063$, $P = 0.183$), failing to support H4a; however, it significantly negatively influenced perceived risk ($\beta = -0.113$, $P = 0.015$), supporting H4b. Furthermore, perceived benefits positively influenced privacy concerns ($\beta = 0.264$, $P < 0.001$), while perceived risks negatively influenced privacy concerns ($\beta = -0.298$, $P < 0.001$), supporting hypotheses H5 and H6, respectively. Privacy concerns significantly and positively influenced willingness to disclose privacy ($\beta = 0.355$, $P < 0.001$), validating hypothesis H7.

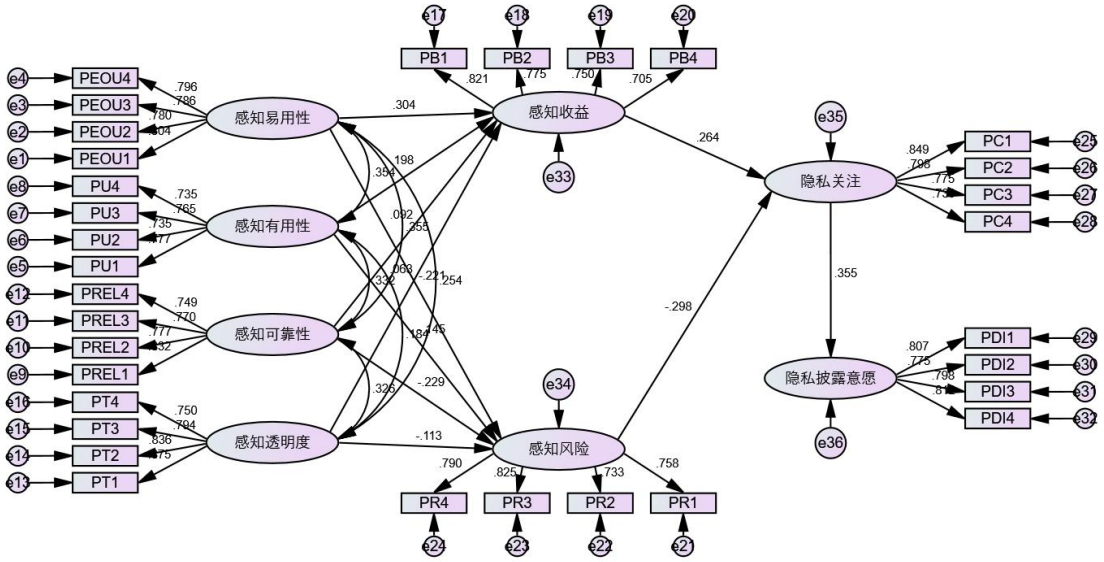

图 2 结构方程路径系数模型图

This study validated the hypothesized relationships among eight variables: perceive d ease of use, perceived usefulness, perceived reliability, perceived transparency, percei ved benefits, perceived risks, privacy concerns, and willingness to disclose privacy info rmation. The research findings are summarized in Table 6.

Table 6 Summary of Research Hypothesis Findings

Number	Content	Result
H1a	Perceived ease of use positively influences perceived benefits	Establishment
H1b	Perceived ease of use negatively impacts perceived risk	Establishment
H2a	Perceived usefulness positively influences perceived benefits	Establishment
H2b	Perceived usefulness negatively influences perceived risk	Establishment
H3a	Perceived reliability positively influences perceived benefits	Not established
H3b	Perceived reliability negatively impacts perceived risk	Establishment
H4a	Perceived transparency positively influences perceived benefits	Not established
H4b	Perceived transparency negatively impacts perceived risk	Establishment
H5	Perceived benefits negatively impact privacy concerns	Establishment
H6	Perceived risk positively influences privacy concerns	Establishment
H7	Privacy concerns positively influence willingness to disclose information	Establishment

Discussion

3.1 Results and Discussion

The differential impact of usage perception on perceived benefits and risks. The s

tudy reveals that both Perceived Ease of Use (PEOU) and Perceived Usefulness (PU) significantly influence perceived benefits and risks, with the direction of influence aligning with the core logic of the Technology Acceptance Model (TAM). This suggests that in AI medical contexts, users' judgments regarding whether a platform is "user-friendly" or "useful" directly determine their assessment of its value and their concerns about risks. An AI medical platform that is easy to operate and addresses practical health issues is more likely to help users perceive benefits—such as personalized diagnosis and time savings—while simultaneously mitigating concerns regarding data breaches or functional failures. This finding is consistent with the research by Palos-Sánchez et al. (2021) on user acceptance of mHealth applications, corroborating the foundational role of technical utility in the digitalization of medical services. Notably, Perceived Reliability and Perceived Transparency only significantly and negatively affected perceived risks, while their positive impact on perceived benefits was non-significant (H3a and H4a were not supported). This result diverges from expectations in trust theory and transparency research (Schnackenberg & Tomlinson, 2016; Esmaeilzadeh, 2019), likely due to the unique nature of medical scenarios. In the context of highly sensitive health information, users' perceptions of "reliability" (e.g., diagnostic accuracy and system stability) and "transparency" (e.g., data usage rules and decision logic) are viewed as "bottom-line requirements" rather than "value-added benefits." That is, users believe a platform should be reliable and transparent by default; enhancing these features does not directly increase perceived benefits, but their absence significantly amplifies risk concerns.

The transmission role of perceived benefits and risks on privacy concern. The finding that perceived benefits negatively influence privacy concern, while perceived risks exert a positive influence, corroborates the applicability of Privacy Calculus Theory in medical contexts (Dinev & Hart, 2006). When users believe that utilizing an AI medical platform yields more accurate diagnostic suggestions and more convenient health management, their concerns over privacy leakage diminish. Conversely, concerns regarding data breaches or misdiagnosis risks intensify privacy concern. This further illustrates that the "benefit-risk" trade-off is more prominent in the medical field, where the ur

gency of health needs may increase user sensitivity to benefits, while the sensitive nat ure of medical data simultaneously lowers their tolerance for risk.

The persistence of the "Privacy Paradox" in medical scenarios. The study found t hat privacy concern positively influences privacy disclosure intention, which contradicts the conventional logic that "higher privacy concern leads to lower disclosure intention, " thus echoing the existence of the Privacy Paradox in medical settings. In the contex t of AI healthcare, users' privacy concern essentially reflects their emphasis on inform ation security; however, this emphasis may actually drive a greater willingness to discl ose information. Users believe that only by providing authentic and detailed health dat a can they receive precise services tailored to their needs. Furthermore, they may use proactive disclosure as a means to prompt the platform to prioritize privacy protection. This result unveils the unique nature of privacy decision-making in healthcare: users' privacy concern is not merely about risk avoidance but rather a rational trade-off aime d at obtaining necessary medical value under controllable risks. Their disclosure intenti on represents a dual demand for both privacy protection and service quality.

3.2 Theoretical Contributions

The theoretical contributions of this study are reflected in the following aspects: Extending the application boundaries of the Privacy Calculus model in medical scenari os. Existing research on privacy calculus has predominantly focused on social networki ng and e-commerce. By introducing this model into AI medical contexts, this study re veals the unique "benefit-risk" trade-off mechanism driven by the sensitivity of medica l data and the necessity of services. Specifically, it demonstrates that perceived reliabil ity and transparency influence privacy decisions primarily through risk perception rathe r than benefit perception, and that privacy concern maintains a positive relationship wi th disclosure intention. This provides a new perspective for the adaptability of privacy calculus in high-sensitivity service scenarios.

Enriching the dimensions of the Technology Acceptance Model (TAM) in privacy research. While TAM traditionally centers on perceived ease of use and usefulness (Davis, 1989), this study incorporates Perceived Reliability and Perceived Transparency as new variables. It identifies their significant impact on risk perception in medical s

cenarios, independent of benefit perception. This indicates that in technological applicat ions involving life and health, "security-related perceptions" (reliability and transparenc y) serve as critical supplementary dimensions of user acceptance, providing empirical s upport for the extension of TAM in high-risk domains.

Revealing the internal logic of the "Privacy Paradox" in medical contexts. This st udy validates the positive impact of privacy concern on disclosure intention, suggesting that in medical scenarios, privacy concern can transform into a driver for conditional disclosure. That is, users utilize privacy concern as a filter to identify reliable AI me dical platforms and proactively disclose information based on trust to obtain service va lue. This offers a new explanatory framework for understanding privacy decision-makin g in highly sensitive fields.

References

Chen Xiaoyan & Gerard Cliquet. (2020). Research on User Privacy Concerns from the Perspective of Privacy Calculus Theory. *Journal of Technical Economics and Ma nagement Research,* (05), 9-13.

Jiang Tingting, Xu Yanrun, Fu Shiting & Lu Wei. (2022). Research on Human-AI Int eraction Experience: Injecting New Momentum into the Development of Human-C entered Artificial Intelligence. Library and Information Knowledge, 39 (04), 43-55.

Zhou Luojing, Shao Yang, Zhang Rui, Li Yunshui, Bao Lei & Xu Daoliang. (2024). Discussion on Ethical Issues and Governance Paths of Artificial Intelligence Appli cations in Smart Healthcare Scenarios. Chinese Hospitals, 28 (02), 38-41.

Zhu Guang, Li Fengjing & Yan Yi. (2022). Research on Privacy Disclosure Behavior in Mobile Healthcare Under the Effect of Paradox Resolution. Information Studies: Theory & Application, 45 (08), 104-114.

Bao Z, Chen W, Xiao S, et al. Disc-medllm: Bridging general large language models and real-world medical consultation[J]. arxiv preprint arxiv:2308.14346, 2023.

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly*, 13(3), 319–340.

Dinev, T., & Hart, P. (2006). An extended privacy calculus model for e-commerce tra nsactions. *Information Systems Research*, 17(1), 61–80.

Esmaeilzadeh, P. (2019). The impacts of the perceived transparency of privacy policies and trust in providers for building trust in health information exchange: Empirica l study.

Featherman, M. S., & Pavlou, P. A. (2003). Predicting e-services adoption: A perceive d risk facets perspective. *International Journal of Human-Computer Studies*, 59(4), 451–474.

Gefen, D., Karahanna, E., & Straub, D. W. (2003). Trust and TAM in online shoppin g: An integrated model. *MIS Quarterly*, 27(1), 51–90.

Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information Syst ems Research*, 15(4), 336–355.

Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995). An integrative model of orga nizational trust. *Academy of Management Review*, 20(3), 709–734.

McKnight, D. H., Choudhury, V., & Kacmar, C. (2002). Developing and validating tru st measures for e-commerce: An integrative typology. *Information Systems Researc h*, 13(3), 334–359.

Holden, R. J., & Karsh, B. T. (2010). The technology acceptance model: Its past and its future in health care. *Journal of Biomedical Informatics*, 43(1), 159–172.

Hu, P. J., Chau, P. Y. K., Sheng, O. R. L., & Tam, K. Y. (1999). Examining the tec hnology acceptance model using physician acceptance of telemedicine technology. *Journal of Management Information Systems,* 16(2), 91–112.

Jeff Smith, Sandra J. Milberg and Sandra J.Information Privacy: Measuring Individuals' Concerns about Organizational Practices Author(s): H. Burke Source: MIS Quarte rly, Vol. 20, No. 2 (Jun., 1996), pp. 167-196.

Khalid, Nazish, et al. "Privacy-preserving artificial intelligence in healthcare: Technique s and applications." *Computers in Biology and Medicine* 158 (2023): 106848.

Palos-Sánchez, P. R., Saura, J. R., & Debasa, F. (2021). Towards a better understandi ng of the intention to use mHealth apps: Exploratory study. *JMIR mHealth and u Health*, 9(9), e27021.

Slovic, P. (1987). Perception of risk. Science, 236(4799), 280–285. SCIRP

Schnackenberg, A. K., & Tomlinson, E. C. (2016). Organizational transparency: A new perspective on managing trust in organization-stakeholder relationships. *Journal of Management*, 42(7), 1784–1810.

Thirunavukarasu A J, Ting D S J, Elangovan K, et al. Large language models in medicine[J]. *Nature medicine*, 2023, 29(8): 1930-1940.

Wu T, He S, Liu J, et al. A brief overview of ChatGPT: The history, status quo and potential future development[J]. *IEEE/CAA Journal of Automatica Sinica,* 2023, 10(5): 1122-1136.

Xu, H., Teo, H. H., Tan, B. C. Y., & Agarwal, R. (2012). Research note—effects of individual self-protection, industry self-regulation, and government regulation on privacy concerns: A study of location-based services. *Information Systems Research*, 23(4), 1342–1363.