Prevalence Overshadows Concerns? Understanding Chinese Users' Privacy Awareness and Expectations Towards LLM-based Healthcare Consultation

Zhihuang Liu, Ling Hu, Tongqing Zhou, Yonghao Tang, Zhiping Cai✉
National University of Defense Technology
{lzhliu, linghu50, zhoutongqing, tangyh, zpcai}@nudt.edu.cn

***Abstract*—Large Language Models (LLMs) are increasingly gaining traction in the healthcare sector, yet expanding the threat of sensitive health information being easily exposed and accessed without authorization. These privacy risks escalate in regions like China, where privacy awareness is notably limited. While some efforts have been devoted to user surveys on LLMs in healthcare, users' perceptions of privacy remain unexplored. To fill this gap, this paper contributes the first user study (n=846) in China on privacy awareness and expectations in LLM-based healthcare consultations. Specifically, a healthcare chatbot is deployed to investigate users' awareness in practice. Information flows grounded in contextual integrity are then employed to measure users' privacy expectations.**

Our findings suggest that the prevalence of LLMs amplifies health privacy risks by raising users' curiosity and willingness to use such services, thus overshadowing privacy concerns. 77.3% of participants are inclined to use such services, and 72.9% indicate they would adopt the generated advice. Interestingly, a paradoxical "illusion" emerges where users' knowledge and concerns about privacy contradict their privacy expectations, leading to greater health privacy exposure. Our extensive discussion offers insights for future LLM-based healthcare privacy investigations and protection technology development.

1. Introduction

Large Language Models (LLMs) are rapidly gaining prominence and popularity, with their applications in the healthcare domain being particularly noteworthy [1]–[3]. Chatbots including OpenAI's ChatGPT, Google's Gemini (Bard), and Microsoft's Copilot (Bing) have further enhanced the accessibility and public interest in LLM-based healthcare consultations [4]–[6]. An intriguing case is ChatGPT's correct diagnosis of a rare disease that had stumped 17 medical professionals [7].

The trend is mirrored in China, where the term "AI-large-scale-model" (literally) was listed among the Top 10 Chinese Buzzwords of 2023 [8], reflecting the widespread adoption of LLM-based chatbots including ChatGPT, Baidu's Ernie Bot [9], and iFlytek's Spark [10]. Due to the large population and insufficient medical resources, people in China frequently use online consultation platforms to seek healthcare information [11]. Statistics show that by the end of 2022, the number of internet medical service users in China reached 363 million, making it the fastest-growing application in terms of user scale in 2022 [12]. Compared to the global market, China is expected to generate the highest revenue in the digital health market, reaching $53.07 billion by 2024 [13][1]. The prevalence of LLM-based chatbots is set to dominate among various online consultation options [4], [14]. It is predicted that from 2023 to 2030, the market size of LLMs in the medical sector in China will grow from $35 million to over $3.08 billion [15].

The unique capabilities of advanced artificial intelligence technologies introduce new privacy risks [16]. For instance, private medical record photos are collected without consent into public datasets to train AI image synthesis models like Stable Diffusion [17]. Similarly, the popularity of LLMs raises more privacy concerns for LLM-based healthcare consultations compared to traditional online consultations. In this context, one may raise the question: ***How do LLMs change the landscape of health privacy?***

Unlike other forms of healthcare consultations, such as searching health-related questions on Google, LLM-based healthcare consultations present unique privacy risks, including: *(1) Increased Exposure of Health Privacy*: Users' sensitive medical information disclosed during consultations is likely collected for future LLM retraining, posing risks of intentional or unintentional access by LLM service providers and numerous global users [18], [19]. Simple data extraction techniques or casual conversations may inadvertently expose and spread health-related data, increasing its vulnerability [18], [19]. *(2) Unpredictable Generative Risks*: The information generated by LLMs is not always accurate or reliable, facing challenges of decision-making opacity and susceptibility to model poisoning [16], [20]–[22]. Users without medical knowledge may encounter fabricated or distorted information during LLM-based healthcare consultations, posing security and privacy threats. For example, incorrect treatments could endanger life, while excessive inquiries could violate health privacy. *(3) Hidden Biases and Non-Compliance*: Healthcare advice generated by LLMs may contain unchecked biases, such as violence, homophobia, and racism [23]. This unfair content can create an unsafe online environment, increasing social tension and individual

1. Prediction data is as of June 3, 2024.

DOI 10.1109/SP61157.2025.00092

psychological stress. Additionally, generated content may infringe copyright laws [24] or fail to comply with the regulations of the user's country [25].

Given that LLM-based healthcare advice is generated in real-time based on user queries, it is challenging to achieve effective real-time regulation compared to information retrieved from Google searches. Therefore, the aforementioned risks become more concealed. Moreover, in China, the privacy issues brought by LLM-based healthcare consultations may be more severe. The inadequate information protection system, lagging legislation, and limited regulatory efforts (illustration in Section 2) make it easier for health privacy violations to occur and escape [26], [27]. Furthermore, the lack of privacy education has led to insufficient awareness and concern among Chinese people regarding health privacy impacts [28], [29].

Several studies have explored user experiences and perceptions of using LLMs in healthcare. Existing research primarily focuses on evaluating LLMs' capabilities in generating medical knowledge and advice [30]–[32], exploring users' perceptions and attitudes towards LLM for healthcare [11], [33]–[36], and the application of LLM in public health support [37] and patient-provider communication [38]. Unfortunately, research so far has not attempted to reveal user privacy awareness and expectations in LLM-based healthcare consultations, particularly in China, where privacy concerns are more acute. In the face of the compelling appeal and unique risks presented by LLMs, understanding user privacy attitudes towards LLM-based healthcare consultations is crucial in guiding the development of privacy-respecting technologies.

Based on the above observations, investigating Chinese users' perceptions of privacy issues in LLMs for healthcare is both necessary and urgent. To this end, this paper takes the first step toward understanding users' perceptions of privacy in LLM-based healthcare consultations. We conduct a survey-based user study in China (n=846), driven by the following research questions (**RQs**):

- **RQ1: Privacy and Technology Awareness.** How would people use LLMs for healthcare consultations? Would they expose personal privacy? What are their attitudes and experiences related to this technology?
- **RQ2: Privacy Expectations.** How acceptable is it for the information involved in LLM-based healthcare consultation to be accessed under different contextual factors? Is people's acceptability related to their backgrounds and attitudes?

To address the above RQs, this paper makes the following contributions:

1) Conducts the first in-depth investigation into privacy awareness and expectations of LLM-based healthcare consultations in China. We design an online chatbot to survey users' privacy awareness during usage, introduce contextual integrity to explore users' privacy expectations, and collect their experiences and feedback.
2) Provides quantitative and qualitative evidence to reveal users' trust, willingness, and concerns about LLM-based healthcare consultations. Our findings reveal that users exhibit high openness and less concern for privacy, particularly in paradoxical situations termed "illusions", which pose risks to health privacy.
3) Serves as a template for extensive surveys and directions for the development of privacy protection technologies. We discuss the challenges of privacy protection in LLM-based healthcare consultations and provide insights based on the results of empirical research.

2. Background and Related Work

Privacy Constructs. This paper discusses constructs such as privacy expectation, privacy attitude, and privacy awareness. Considering that the same privacy construct often has different descriptions of the underlying phenomenon in various literatures [39], [40], to avoid confusion, the main privacy constructs used in this paper are defined as follows to ensure consensus among readers: *(1) Privacy awareness*: Understanding and consciousness of the importance of personal privacy protection and the potential risks of personal information in specific privacy-related situations. The terms *perception* and *perspective*, as used in the paper, have very subtle differences from *awareness*. We use *perception* to describe a more general understanding or direct sensory experience, *perspective* to describe understanding from different dimensions or angles, and *awareness* to describe deeper, underlying consciousness and inner views. *(2) Privacy expectation*: The degree of acceptability or the desired level of privacy protection in anticipated specific privacy-related situations. *Privacy preferences* have a very similar meaning to this construct [40]. We use the term *privacy expectation* to maintain consistency with studies based on contextual integrity [41]–[44]. These studies also often use the term *privacy norm* to refer to a similar meaning, and so does this paper. *(3) Privacy attitude*: An individual's predisposition and stance towards different privacy-related situations. *(4) Privacy concern*: The anxiety and worry about specific privacy-related situations. *(5) Privacy knowledge*: An individual's understanding and consciousness of concepts, regulations, technologies, and practices related to privacy issues.

Privacy as Contextual Integrity. The Contextual Integrity (CI) theory developed by Helen Nissenbaum [45] provides a framework for understanding privacy norms and expectations. CI defines privacy based on the appropriateness of information flows within specific contexts. Each information flow is described by five parameters: (1) the *subject* of the information, (2) the *sender* of the information, (3) the *recipient* of the information, (4) the *attribute* or type of information, and (5) the *transmission principle* or condition from sender to recipient. Changes in these parameters can result in different information flows, potentially leading to deviations in privacy expectations within a specific context, thereby affecting acceptability.

Previous research has extensively employed CI to reason and uncover privacy norms across various contexts [29], [41]–[44], [46]–[51], assessing privacy expectations, privacy

regulations, or exploring tools that meet user privacy needs. Apthorpe et al. [42] used CI to evaluate whether the U.S. Children's Online Privacy Protection Act (COPPA) aligns with parents' privacy norms regarding smart toy data collection. Minaei et al. [44] employed CI to investigate users' privacy expectations for deletion events on social platforms. Kablo et al. [43] applied CI to understand neuroprivacy expectations, laying the groundwork for designing privacy-respecting neurotechnology. As a core aspect of this paper, CI is applied to explore users' privacy expectations regarding information flows in the emerging scenario of LLM-based healthcare consultations.

User Study on LLM Applications in Healthcare. Given the increasing application and research of LLMs in healthcare [4], several empirical studies have focused on user perception. Leveraging user-based artificial analysis and review, researchers can evaluate the medical capabilities of LLMs [30]–[32]. Moreover, previous research has also investigated users' perceptions and attitudes. Choudhury et al. [33] collected responses from 607 participants in the United States, particularly those who use ChatGPT for healthcare queries, to understand users' views on the effectiveness, credibility, and safety of ChatGPT in the healthcare domain. Nov et al. [34] conducted a study where participants were asked to identify responses generated by an LLM-based chatbot regarding electronic health records. Chuan et al. [35] created a chatbot embedded in a health information website to conduct medical interviews with participants, including embarrassing questions, and explored users' self-disclosure behaviors. Xiao et al. [11] used a combination of surveys and interviews to investigate how and why the public uses LLMs in healthcare. Similarly, Raina et al. [36] employed mixed methods to survey general users and healthcare professionals in India, aiming to gather insights on utilizing LLMs in healthcare.

Unfortunately, the aforementioned works have not centered on the crucial issue of privacy in user studies. Although Xiao et al. [11] and Raina et al. [36] briefly touch on privacy concerns in their discussions, neither set out to collect in-depth user perceptions with a focus on privacy issues. Our work, with a core emphasis on understanding users' privacy needs, contributes to this area. In fact, recent work [52] has unveiled users' privacy concerns regarding LLM-based conversational agents. However, as noted in their limitations, users' risk perceptions and privacy-seeking behaviors related to LLM-based conversations change with different contexts. Unlike the broad scope of privacy concerns, this paper aims to delve into the awareness and expectations of Chinese users in the specific context of LLM-based healthcare consultations. This issue is worth exploring due to the sensitivity of health information and the associated life-threatening health risks.

User Study on Privacy in China. Although user studies concerning security and privacy issues are typically conducted among populations in Western countries such as the United States and various European nations, several studies have expanded their scope beyond these countries to include China [28], [29], [53]–[57].

Specifically, user surveys conducted in China have unveiled unique findings regarding privacy awareness. Wang et al. [28] observed that, compared to American respondents, Chinese participants were significantly more willing to share data for online behavioral advertising (OBA), with fewer specific concerns. They suggested that the later development of privacy concepts and regulatory frameworks might contribute to the lower level of concern about online privacy among Chinese individuals. Utz et al. [29] found that among participants from the United States, Germany, and China, Chinese users exhibited the highest acceptance and least privacy concerns towards "corona apps". Similarly, Huang et al. [27] noted that Chinese users' perceptions of privacy protection starkly contrast with Western concerns about privacy risks. Feng et al. [26] argued that China's legal system for data protection is lagging, yet the Chinese government and legislature are increasingly prioritizing personal information and privacy protection.

In fact, the U.S. federal government officially enacted the Health Insurance Portability and Accountability Act (HIPAA) as early as 1996, while China only had two broad guiding documents before 2016, such as the Guiding Opinions on Information Security Level Protection Work in the Health Industry, which were difficult to implement effectively. In terms of personal information protection, the significant gap in China's legal system was not addressed until the Personal Information Protection Law was formally implemented at the end of 2021 [58]. ***How aware are Chinese users of privacy issues in LLMs for healthcare under these circumstances?*** Our research will shed light on this question.

3. Methodology

3.1. Survey Instrument

The survey instrument consists of online experiences and questionnaire surveys. Initially, an LLM-based healthcare chatbot is designed for an online experiment and presented to users in Chinese[2]. In the questionnaire, Part I inquires about the users' experiences consulting with the chatbot for medical advice. Subsequently, Part II defines 144 CI-based information flows to test users' privacy expectations [41]–[44] when using LLM-based healthcare consultation. Part III probes into users' attitudes and previous experiences, followed by demographic questions. More details about the survey instrument can be found in Appendix A.

3.1.1. Healthcare Chatbot. We design the healthcare chatbot for the following reasons: (1) Considering that some people may not have experience using LLMs for healthcare consultations, we developed a healthcare chatbot to mitigate users' unfamiliarity with this process. (2) To observe users' awareness when using a chatbot for healthcare consultations.

2. The deployed system is available at http://healthllm.top/LLMHPri/encindexzh/, and the English version is available at http://healthllm.top/LLMHPri/encindexen/.

This online experiment allows us to introduce simulated risk in a controlled manner, as is common in the field of *Usable Privacy and Security* [59].

This chatbot is built on GPT-3.5[3]. Although many domain-specific LLMs have gained popularity in the medical field, general-purpose chatbots like ChatGPT remain the most widely used and accessible LLM applications in daily life. Furthermore, employing ChatGPT ensures consistency with related studies [35], facilitating replicability in this field, while leveraging its strong medical capabilities [7], [18], [20], [32]. Without loss of generality, we follow OpenAI's prompt engineering guidelines[4] to design the prompt that includes the identity, intent, and behavior of the model. The prompts are iteratively evaluated and optimized through internal testing and pilot studies. The designed prompts mainly cover several aspects: *Identity*: an experienced and trustworthy healthcare professional. *Intent*: to provide reliable and impressive responses to users' healthcare-related inquiries. *Behavior*: consider the conversation history (if any); provide personalized advice if the user provides information; further inquiries if the user's question is related to personal health and requires a prescription.

Before initiating queries, we outline the precautions and risks associated with using the healthcare chatbot. We advise users to consider their questions in advance and then decide whether to input basic information such as age and gender for personalized advice. We also remind users with medical backgrounds to critically evaluate the responses or advice generated by the model. In the chat interface, the chatbot begins with an initial message instructing users on how to use the service. Three easily recognizable general health-related questions are provided above the input box to allow users to initiate consultations directly. After receiving a query, the chatbot displays the response letter by letter and updates suggested follow-up questions above the input box. Each participant is allowed to ask up to 10 queries. In addition, the open-access deployed system link and the open-source code[5] will facilitate further exploration of details such as the prompts used and the consultation queries.

3.1.2. Questions of Survey. We utilize the Wenjuanxing platform (wjx)[6], a popular survey platform in China [60], similar to Qualtrics[7], to create our questionnaire. The survey was developed by native Chinese speakers and covered the following categories.

Part I: Awareness During Consultation (RQ1). The survey begins by asking users about their experiences with healthcare chatbot consultations. Initially, users are requested to recall the types of questions they asked during healthcare consultations, whether they provided basic information and the reasons behind it. We then inquire about any dissatisfaction with the consultation. Furthermore, we seek to understand whether users would verify and adopt the responses and suggestions mentioned by the chatbot. Lastly, we ask users if they feel their privacy was compromised during the consultation and, if so, to further describe the privacy aspects they believe could have been exposed.

Part II: Privacy Expectations (RQ2). Considering real-world healthcare consultation scenarios and drawing on previous research [41]–[44], along with feedback from pilot studies, we design contextual integrity questions. After filtering CI parameters, 144 information flows related to CI are generated, with the final CI parameters presented in Table 1. Both *Sender* and *Subject* are fixed as the user, as LLM-based healthcare consultations are typically initiated by users themselves. We identify four representative entities as *Recipients* of LLM-based healthcare consultation information. Additionally, we categorize four different levels of *Attributes* based on the healthcare scenario, including sensitive healthcare information like the user's mental health and medical information. Finally, we define 10 different *Transmission Principles* involving consent, notification, storage, usage, privacy policies, etc., with the *null* transmission principle serving as a control to generate information flows without specific conditions. The selected CI parameters are not exhaustive. Specific or detailed principles, such as anonymized and encrypted transmission, have been excluded to reduce the burden on participants in understanding technical terms, distinguishing details, and evaluating information flows.

Considering that 144 questions might be overwhelming for individual participants (as indicated by the *Pilot Studies* in Section 3.2.1.), we divide the 144 information flows into 20 distinct matrix-like blocks. In 16 of these matrix-like blocks, each contains the same attribute and recipient, with different information flows generated by changing the transmission principle (see Figure 8 in Appendix A). The remaining 4 matrix-like blocks have varying attributes, each with four recipients, acting as information flows for the *null* transmission principle (see Figure 7 in Appendix A), similar to the approach by Apthorpe et al. [41], [42]. This division aims to reduce cognitive fatigue among participants. Each participant is randomly assigned two matrix-like blocks with the same attribute, one containing *null* transmission principle information flows with different recipients (like Figure 7), and the other containing up to nine information flows with different transmission principles (like Figure 8).

Participants are asked to rate the acceptability of each CI information flow on a five-point Likert scale: Completely Acceptable (2), Somewhat Acceptable (1), Neutral (0), Somewhat Unacceptable (-1), Completely Unacceptable (-2), with the corresponding values termed *acceptability scores*. Following the two CI-based blocks, we adopt the methodology of Kablo et al. [43] to set questions exploring whether users independently evaluate different transmission principles, i.e., whether they always assume that all information flows are predicated on the first principle "if the user has given consent". Different answers to this question are consequently used for grouping in the statistical tests. Lastly, we add one attention-check question.

3. The latest free version of ChatGPT at the time of this study.

4. https://platform.openai.com/docs/guides/prompt-engineering

5. https://anonymous.4open.science/r/LLMHealthPrivacy_UserStudy-F25F

6. https://www.wjx.cn/

7. https://www.qualtrics.com/

TABLE 1: Contextual Integrity parameters selected to generate information flows of LLM-based healthcare consultations. The user's family members and healthcare providers correspond to 8 Transmission Principles, the remaining two Recipients correspond to 10 Principles, and finally form 144 information flows (4×8+4×8+4×10+4×10).

Sender	Recipient	Subject&Attribute	Transmission Principle
user itself	the user's family members	the user's basic information	if the user has given consent
	healthcare providers	the user's lifestyle	if the user is notified before collection
	government agencies	the user's mental health information	if information is kept confidential and not stored
	LLM service providers	the user's medical information	if information will be stored
			if information is used for health monitoring
			if information is shared with others (beyond the specified recipient)
			if it complies with information protection regulations
			if information is provided for academic research
			if information is used in public health surveys
			if used for information analysis and service improvement
			null (no principle)

Part III: Attitudes and Previous Experiences. We include this part in **RQ1** because, by investigating users' past experiences and overall attitudes, we aim to draw conclusions regarding privacy and technology awareness. Participants answer questions about their previous use of LLM technology and their previous experiences with online healthcare consultations. Then, we ask participants whether they are willing to use reliable LLMs for healthcare consultations in the future and select their reasons for this preference. Finally, participants self-assess their understanding of and concern for health privacy and describe any encountered health privacy breaches.

Demographics & Background. The final part of the survey poses a series of demographic and background questions to understand the representativeness of the sample and to consider demographic variables in the analysis. A free-text box is provided for participants to share any thoughts or suggestions, particularly regarding privacy.

Note that the questionnaire does not provide a unified description of privacy or health privacy to ensure a common understanding among participants, and at most, it only provides examples to help users recall potential privacy breaches as much as possible. This approach aims to assess participants' natural and pre-existing privacy awareness, aligning with several studies [43], [44], [61].

3.2. Survey Deployment

We integrate the constructed chatbot with the designed questionnaire into a prototype system, embedding the questionnaire within the system via an iframe. The homepage of this system provides a basic introduction to the survey and an informed consent form. Users are required to read and agree to the informed consent form before participating in the survey. The developed system is hosted on Alibaba Cloud[8], with subsequent pilot studies and the formal survey conducted there.

3.2.1. Pilot Studies. Before deploying the survey, we conducted two pilot studies to assess the research procedure, determine the average participation time, and test the comprehensibility of the questions. The first pilot invited 20 Chinese participants from the researchers' social circles, including 10 with computer science background, 3 from Chinese language majors, 4 with medical background, one aged between 35-44, and one over 50. Feedback highlighted issues with overly lengthy and complex questions, excessively formal and technical language, excessive questions, and UI design.

The principal researcher and other team members reviewed the pilot study results and determined adjustments, including: (1) optimizing system design by tailoring chatbot prompts for specificity, adjusting chat interface buttons and information cues; (2) reducing the number of survey questions, particularly those about CI information flows, resulting in each participant responding to 2 CI-based blocks instead of 5, with fewer information flows within each block; (3) simplifying and popularizing question and option descriptions, avoiding overly professional and formal expressions, and using easily understandable Chinese terms, e.g., changing "if the user has given verifiable and revocable consent" to "if you have given consent" (using "the user" instead of "you" in this paper). Specifically, we described LLM as "AI-large-scale-model" and added friendly explanations to align with popular terminology in China and to ensure comprehension by participants, especially those without a computer science background or older participants.

After the first pilot participants indicated these changes were sufficient, we conducted a second pilot study. We asked friends and colleagues to share the test within their social circles, gathering results from 30 participants of diverse backgrounds, all completing our survey within 10 minutes. Feedback indicated that the majority could understand and complete the survey.

3.2.2. Recruitment. The survey was conducted over two weeks starting in March 2024. Similar to [55], [57], the researchers first posted recruitment information and survey links on various types of chat groups within mainstream Chinese social applications like WeChat and QQ, requesting friends to further spread the survey through WeChat Moments and QQ Statuses[9], ensuring reach beyond our social networks. Consistent with many studies [41], [44],

8. https://www.alibabacloud.com

9. Commonly used spaces for sharing and communicating in China.

we avoided mentioning our focus on security and privacy to reduce sample bias. All Chinese-speaking residents of China aged 18 and over are eligible to participate, with particular efforts to reach out to those with medical backgrounds or older participants. To further diversify the sample, recruitment posts were published on more public social platforms including Xiaohongshu (referred to as "Chinese Instagram"), Sina Weibo (microblog platform), and Douyin (Chinese version of TikTok), each boasting over 100 million monthly active users. Interested users contacted the poster to receive the participation link.

We determine the sample size based on several considerations: 1) exceeding 10 times the number of questions; 2) referencing prior studies [29], [41]–[44]; 3) moderately increasing the sample size; and 4) ensuring sufficient responses for each CI-based block. The between-subjects design, similar to [41], [42], [44], is chosen to reduce participant fatigue and enhance response validity. The large sample size helps mitigate the typical impact on statistical power associated with between-subjects designs. In total, we received 1,106 complete responses, with 846 valid ones. The final sample (see Section 3.2.4) reflects a diverse range of participants in terms of age, gender, education, and region. Each information flow is evaluated at least 40 times, exceeding the counts reported in [41], [42], [44]. The participation time begins only when participants click '*Agree and Enter the Survey*', ensuring they have sufficient time to read the informed consent. The average completion time for the survey is 7.14 minutes, with participants receiving a 7 RMB reward (approximately $1, $8.12/hr), distributed via WeChat red packets through the wjx platform. Additionally, users spend an average of 2.42 minutes interacting with the LLM, which is sufficient to complete more than 3 inquiries, according to pilot studies. The compensation standard is comparable to related studies [44], [62], [63], and no participants expressed concerns regarding inadequate compensation.

3.2.3. Quality Control. To address potential dishonest or careless responses, we set attention-check questions and reminders to ensure response quality. First, we assign numbers to the users who enter the system in order and remind the users to remember their numbers at the end of the chatbot conversation, requiring users to fill in their ID number in the first question of the questionnaire. To assist those who might forget their number, a 15-second reminder is displayed at the top of the survey interface. The ID serves both as a reminder for users to focus and as a means to align the same participants to calculate the total participation time. We divide the questionnaire into four pages according to the structure described in Section 3.1.2, reminding users to focus and indicating their progress on each page to minimize fatigue. After answering CI information flow questions, users are asked, "*Which option is not mentioned above?*". After participants' informed consent, we temporarily collected their IPs to prevent duplicate participation, and also gathered the WeChat openid (an anonymized identifier) during red packet distribution to identify repeat responses attracted by the reward; such responses were not compensated nor included in the collected data. We fully deleted IP and openid information before the formal analysis, with detailed ethical considerations described in Section 3.4.

3.2.4. Participants' Demographics. We received 1,106 completed responses, with 256 responses discarded for one or more of the following reasons: the number entered falls outside the system's assigned number range; failed attention checks; excessively short completion times; and identical or meaningless CI information flow responses. We then reviewed and removed responses with garbled or false text replies (1) and those outside China (3). The final sample is n=846, with each CI information flow receiving at least 40 responses.

Our sample covers all provinces in Mainland China and 173 cities, mostly from the eastern and central regions (75.3%), reflecting the concentration of many Chinese people in these areas for study and work [64]. The participant gender distribution is nearly balanced, with 49.5% identified as female, 48.6% as male, and 1.9% as others[10]. Similar to related studies [43], [44], the sample is predominantly young, with 78.8% under 35 years, 12.4% aged between 35-44, 5.2% between 45-54, and the remainder 1.2% over 55. In terms of education, 44.2% of participants had a bachelor's degree, 19.3% had a master's degree or higher, and 18% were undergraduates. 54.1% of participants reported having study experience in IT-related courses or IT work background, and 42.9% had education experience related to data security or privacy. Additionally, 15.6% of participants had a medical background, and 21.5% had a healthcare professional or personal physician readily available for queries. Detailed demographic data can be found in Appendix B.

3.3. Data Analysis

Most responses to the questionnaire were translated into English for analysis. Two researchers employed a forward-backward translation method. Discrepancies were addressed through discussion, and the final version was reviewed by the research team. Free-text responses were reviewed, coded, and then translated into English for collaborative discussion and reporting.

Quantitative analysis methods. We employed statistical hypothesis testing to investigate privacy norms in LLM-based healthcare consultations. The five-point Likert scale was converted into ordinal variables and treated as continuous data. To assess participants' acceptability tendencies regarding information flows, the Sign Test was applied to evaluate the central tendency of 144 information flows, accounting for multiple comparisons using the Bonferroni correction method, setting the threshold to 3.47e-04 (0.05/144). We also utilized non-parametric Wilcoxon signed-rank tests to explore the influence of CI parameters, participant demographics, or self-reported factors.

10. It is recommended to refer to [65] using a checkbox format containing the following five options: *woman, man, nonbinary, prefer not to disclose, and prefer to self-describe*.

Specifically, to assess the impact of transmission principles, following [41], [43], we compared the acceptability scores between the same attributes and recipients but with *null* and *non-null* transmission principles, using the *null* transmission principle as a baseline. We conducted 128 Wilcoxon tests for the different combinations of four attributes and four recipients, thus adjusting the standard significance threshold to 0.00039 (0.05/128) based on the Bonferroni method. Then, we conducted 10 Wilcoxon tests to compare the impact of different demographic groups on acceptability scores, setting the threshold to 0.005 (0.05/10) to account for Bonferroni correction. Furthermore, 8 Wilcoxon tests were carried out to compare the impact of different attitude tendencies on acceptability scores, with the threshold set to 0.00625 (0.05/8) for Bonferroni correction, as 8 attitude tendencies groups were used. Additionally, we conducted several other Wilcoxon tests to ensure that statistical results are included when making comparisons and drawing general conclusions. Notably, each participant responded to two CI-based blocks, one of which included the acceptability scores under the *null* transmission principle for 4 recipients. We selected the score with the same recipient as the other block.

Qualitative analysis methods. For free-text responses obtained from the survey, thematic analysis [66] and inductive coding [67] are used to reveal users' perceptions. Native Chinese speakers with data analysis experience participated in the coding. A primary researcher read the responses and iteratively generated a codebook, after which another researcher independently coded the free-text responses based on this codebook. Cohen's Kappa κ was used to measure inter-coder agreement and reliability, achieving $\kappa > 0.81$ for different open questions, indicating high consistency. The coders discussed and resolved discrepancies for different cases, and all researchers determined the themes corresponding to the codes through meetings.

3.4. Ethical considerations

Our institution's Institutional Review Board (IRB) reviewed and approved this project. Before the survey, an informed consent form notified participants about the survey content, collected information, potential risks, and their rights. All responses were anonymous, and participation was entirely voluntary, with participants free to withdraw at any time during the study.

Users consult LLMs for medical advice, which forms part of our study to observe their awareness when using a chatbot for healthcare consultations. The risks and impacts associated with such designs are difficult to fully eliminate in simulated testing within this field [59]. To minimize potential harms in the study, several measures were implemented: (1) *Warnings and voluntary consent*. Clear warnings were displayed on the informed consent page, on the pre-chat page, and in the conversation, reminding participants to consult a doctor before acting on chatbot advice. Users were informed they must agree to OpenAI's terms and privacy policy, as the LLM is GPT-based. (2) *Minimal data collection*. IPs were temporarily collected for uniqueness, deleted post-survey, and WeChat openids were gathered for rewards, ensuring anonymity. Only random user numbers and session durations were recorded during consultations, with conversation data was deleted at the end of each session. (3) *Monitoring and data security*. No abnormal traffic on the deployed website was detected using Alibaba Cloud security tools. We deleted stored databases on Alibaba Cloud and wjx after the survey, redirected the website, and stored analyzed data on password-protected local devices accessible only to study authors.

Note that to avoid ethical concerns, most *Usable Privacy and Security* research does not use deception to expose participants to simulated risks [59]. However, some research topics may require limited deception to approximate reality. We use a partial disclosure approach to risk, similar to [68]. For instance, we provided a link to OpenAI's privacy terms instead of explicitly stating that users' input data could be reviewed and used for model training. This setting aligns with reality, as whether to thoroughly read the specific terms depends on the users themselves.

Ultimately, no participants raised concerns about compensation or the risks of participation in their final free-text responses, nor did they contact us or the IRB for feedback. Upon completing the survey, we consistently invited participants to report any risks associated with their involvement. Furthermore, the post-study education was disseminated through the same recruitment channels, informing participants about the limitations and risks of LLM-generated advice, such as potential inaccuracies, unknown sources, and unclear responses. Key study findings were also shared, along with helpful links for further education.

4. Results

4.1. RQ1: Privacy and Technology Awareness

Analyzing users' responses to the online consultation experiences (Part I) as well as responses about attitudes and previous experiences (Part III), we observed the following key findings.

4.1.1. Participants Seek Personalized, Clear and Reliable Advice. In online LLM medical consultations, the majority of participants (381/846, 45%) reported consulting on personal health issues, slightly more than those who consulted on general health knowledge (333/846, 39.4%). As shown in Figure 1, 619 participants (73.2%) provided personal information such as age, primarily seeking personalized advice, reflecting a widespread desire for customization.

All participants were asked about any dissatisfaction with their consultation experience. We offered five different options (including "None") based on pilot study findings, with an additional "Other" option for free-text responses. After coding the responses (Cohen's κ=0.85), we added six additional reasons to the list (including "Other"), as shown in Table 2. The primary dissatisfaction reported was regarding the quality and reliability of responses, with 25.8%

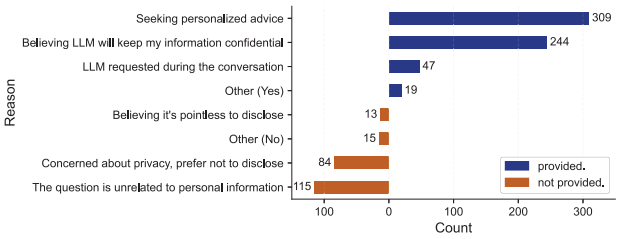


Figure 1: Reasons for participants providing or not providing basic information.

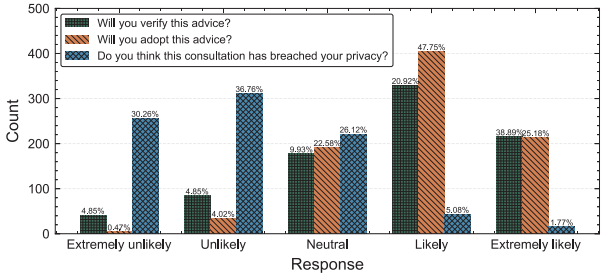


Figure 2: Comparison of responses on user awareness.

TABLE 2: Dissatisfaction with the online consultation.

Dissatisfaction	Freq. (%)
None	482 (57.0%)
Unclear response or untargeted	218 (25.8%)
Unknown source or concerns about accuracy	151 (17.8%)
Chatbot overly asks for personal information	31 (3.7%)
Slow response	17 (2.0%)
Other	9 (1.1%)
Lengthy or repetitive responses	8 (0.9%)
Uncomfortable response	7 (0.8%)
UI design	6 (0.7%)
No further inquiries	4 (0.5%)
Not comprehensible enough	3 (0.4%)

(218/846) of users finding the LLM's answers unclear or not personalized enough, appearing untargeted; 17.8% were concerned about the lack of clear sources, raising doubts about the accuracy.

It is noteworthy that the pursuit of personalized advice is often linked with compromises in privacy [69]. The analysis in this part indicates that users may overlook the relationship between personalization and privacy, reflecting either their lack of concern for privacy or their trust in popular LLMs, as further analyzed subsequently.

4.1.2. Participants Willing to Trust LLMs. It is notable from Figure 1 that the second most common reason participants provided their basic information was trust in the LLM to keep their information confidential, chosen by 244 participants. Additionally, 47 reported providing information in response to the LLM's inquiry. In Table 2, 57% (482/846) of the participants found no dissatisfaction. Furthermore, Figure 2 presents participants' likelihood of verifying and adopting advice and their perception of privacy breach risk. Participants tended to verify and **adopt advice** (selecting *Likely* and *Extremely likely*), reaching 59.8% and **72.9%**, respectively. Most participants (67%) believed their privacy was unlikely to be breached (selecting *Extremely unlikely* and *Unlikely*) during the healthcare consultation experience.

4.1.3. Limited Participants Express Privacy Concerns. Preliminary internal tests and pilot studies indicate that the chatbot occasionally asks for age, gender, and past medical history. Consequently, 3.7% (31/846) in Table 2 of the participants were dissatisfied with the chatbot overly asking for personal information, likely feeling an intrusion into their privacy. Moreover, 58 participants who felt privacy might be breached during the consultation experience (selecting *Likely* and *Extremely likely*) were further asked to specify the privacy they thought could be compromised. Disregarding 25 responses that were empty or stated "none", the remaining responses were coded (Cohen's κ=0.93), revealing three different themes. Participants most commonly believed that *Basic information* such as age, gender, and career could be breached (83.3%), followed by *Healthcare information* (10.4%) and *Issues inquired about* (6.3%). This indicates that while some participants discussed their symptoms or other health privacy issues and expressed concerns, overall, participants were not highly sensitive to privacy issues in LLM-based healthcare consultations.

4.1.4. Technology Experiences. Among the 846 participants, 109 (12.9%) indicated no experience with LLMs at all; however, 553 (65.4%) had experience using LLMs, and among these, more than half (335/553, 60.6%) had used them for healthcare consultations. These results greatly surpass the 7.2% (44/607) usage rate for health-related queries using ChatGPT reported in a 2023 U.S. survey [70], but are still below the 73.7% (123/167) reported in a 2024 survey [11], highlighting the necessity of conducting up-to-date user surveys. Of the 511 participants without LLM-based healthcare consultation experience, 331 (64.8%) reported having consulted healthcare information online, indicating that at least 666 of the 846 participants (78.7%) had consulted healthcare issues online. It can be anticipated that the use of LLM-based healthcare consultations is likely to become a prevalent trend in the future. This hypothesis is further supported by Figure 3, where **a majority of participants (654/846, 77.3%) expressed their intention to use reliable LLM-based healthcare consultation services** in the future.

4.1.5. Attitudes Evident in Choices. We convert the scores from the four five-point Likert scales in this part to a range from -2 (*Strongly disagree*) to 2 (*Strongly agree*) for comparative analysis, as shown in Figure 3. The majority of individuals (748/846, 88.4%) expressed concern for health privacy and indicated a high likelihood (77.3%) of using reliable LLM-based healthcare consultation services in the future. However, less than half of the participants (383/846, 45.3%) believe they understand health privacy, with only 101 participants strongly agreeing that they do, indicating a significant portion of users lack a clear concept of health privacy. Additionally, the view that consulting healthcare questions online poses a greater risk of privacy breach was

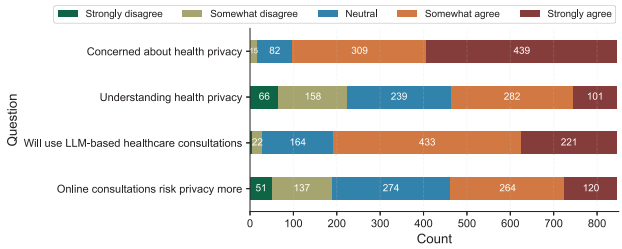


Figure 3: Distribution of user responses to five-point Likert scales questions in Part III.

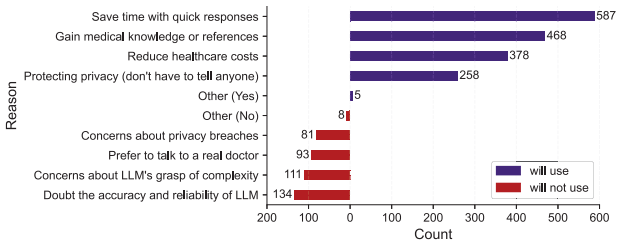


Figure 4: Reasons for participants' willingness or unwillingness to use LLM-based healthcare consultations.

not overwhelmingly endorsed, receiving agreement from only 384 participants (45.4%).

Further, we inquired why participants chose to use LLM-based healthcare consultation services (those selecting *Somewhat agree* and *Strongly agree*) or why they were disinclined to use such services (those selecting *Strongly disagree*, *Somewhat disagree*, and *Neutral*). We provided multiple choices and the distribution of reasons in the responses received is shown in Figure 4. Observably, on the positive side, saving time, increasing medical knowledge, and reducing healthcare costs were common reasons. Additionally, 258 participants chose "*Protecting privacy (don't have to tell anyone)*", accounting for 39.4% of those inclined to use the services, with some believing that conveying health concerns to a machine rather than a person can avoid embarrassment. On the other hand, concerns about accuracy and reliability were the main reasons for participants' reluctance to use these services. Nevertheless, only 81 instances were concerned about privacy breaches.

The analysis in Sections 4.1.1-4.1.5 indicates that many participants exhibit trust in LLMs and their generated healthcare advice. This trust may stem from the positive impressions and reliance on LLMs created through their promotion [11], [52], [70]. Consequently, the prevalence of LLMs likely amplifies health privacy risks by increasing users' curiosity and willingness to engage with such services.

4.1.6. Recommendation Algorithms Challenging Health Privacy. Most participants (604/846, 71.4%) reported that they had not experienced health privacy breaches. Of the 157 participants who reported experiencing privacy breaches, 49 provided further descriptions of their experiences. We coded the substantive descriptions from 48 responses (Cohen's κ=0.81), identifying five categories of privacy breach descriptions. Most responses indicated a sense of privacy invasion due to **Recommendation systems** (43.5%), mentioning examples such as *product recommendations*, *cross-app recommendations*, and *search suggestions*. For instance: *"After searching for information on orthodontics, sports, and physiotherapy, I started seeing ads for related products on Baidu, WeChat, Taobao, and Pinduoduo" (P283)*[11]. The next top category involves **Communication** (30.4%), including *text marketing*, *phone calls*, and *phone follow-ups*. Then comes **Advertisement** (17.4%) related to the consultation content. These ads might be promoted through phone calls, text messages, or even using patients' treatment cases for publicity. Additionally, some responses mentioned being subjected to *nuisance calls* or *text message spam*. More alarmingly, a few participants revealed incidents where their medical conditions became known to others.

In the era of LLMs, data is increasingly collected for model training and faces greater exposure risks. Once users' health information is linked with recommendation algorithms, the challenges to health privacy become more severe.

4.2. RQ2: Privacy Expectations

Subsequent analysis reveals how users' acceptance of their LLM-based healthcare consultation information being accessed correlates with various factors, offering insights into their contextual privacy norms. The following subsection elaborates on the significant findings from this analysis.

4.2.1. Average Acceptability Scores and Tendency Comparison. Figure 5 shows the average acceptability scores for different recipients under various transmission principles obtaining different attributes. Scores range from -2 (dark red) to 2 (dark blue), with lower scores indicating less acceptability. We also tested the percentage of acceptability (scores of 1 or 2) and unacceptability (scores of -1 or -2) for each type of information flow. The results indicate that the trends reflected by the comparison of tendency percentages largely align with those shown by the average acceptability scores. Therefore, the following sections generally omit detailed discussions of proportion comparisons.

The Sign Test was applied to examine the 144 CI-based information flows independently, with the Bonferroni correction applied (threshold set at 3.47e-04). The results indicate that 85 flows show a significant trend toward acceptability (59.0%), 17 flows lean significantly toward unacceptability (11.8%), and 42 flows exhibit a significant trend toward neutrality (29.2%). Intuitively, the acceptability scores under different transmission principles exhibit variance, especially lower acceptability under "if data will be stored" and "if data is shared with others", whereas the column "if the user has given consent" shows higher acceptability scores. We also observed a difference in acceptability scores across different recipients. Participants found it more acceptable for

11. Taobao and Pinduoduo are popular Chinese online shopping platforms.

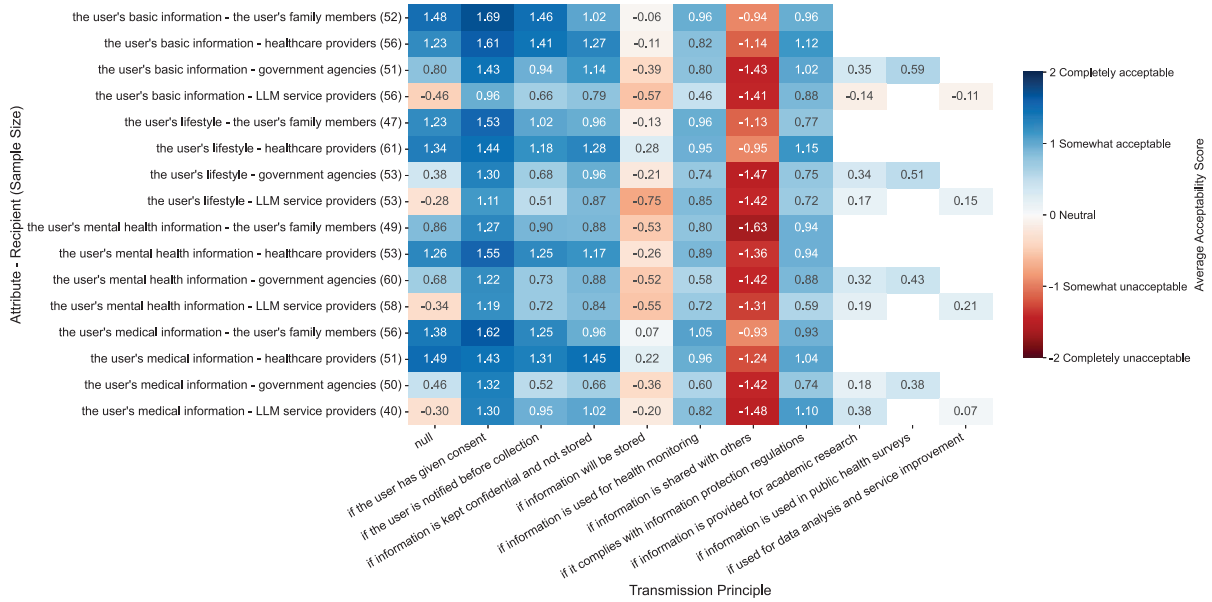


Figure 5: Average acceptability scores for information flows grouped by attribute, recipient, and transmission principle. Each small grid corresponds to a specific contextual information flow, with the number in parentheses following Attribute-Recipient indicating the frequency of responses for that category of information flow. Acceptability scores range from -2 (completely unacceptable) to 2 (completely acceptable).

family members and healthcare providers to access their information, with average scores and acceptable/unacceptable ratios of 0.68 (63.7%/22%) and 0.78 (68.1%/17.5%), respectively. In contrast, acceptability was lower for government agencies and LLM service providers, with scores of 0.4 (55.2%/24.8%) and 0.21 (49.1%/31.2%). Six Wilcoxon tests (p=.0083) revealed significant differences when comparing family members to government agencies or LLM providers, and healthcare providers to the same (p <.0083). This pattern persisted under the *null* principle, with LLM service providers consistently rated as unacceptable (scores below 0). Regarding the acceptability of different attributes, mental health information scores the lowest on average at 0.37, followed by basic information (0.44), lifestyle (0.45), and medical information (0.47), without significant differences (p >.0083).

Interestingly, all recipients and attributes received positive scores on average. Additionally, participants were more open to healthcare providers and medical information, with average acceptability scores higher than those for family members and basic information. We speculate this is due to the survey's focus on healthcare consultations. Also noteworthy is that information flows under the principle of "if it complies with information protection regulations" (tendency ratios 70.8%/10.1%) scored on average 0.46 lower than the consent (87.6%/3.6%) category, indicating a significant difference (p=.000031) and suggesting a lack of trust in privacy policies.

4.2.2. Principles Impact Acceptability. We assessed the impact of adding specific transmission principles to unconditional information flows for each combination of recipient and attribute. We calculated the percentage of information flows showing significant differences from their corresponding *null* transmission principles (p <.00039), as shown in Figure 6. It was observed that "if information is shared with others" invariably resulted in acceptability scores significantly different from the *null* principle, followed by "if information will be stored" at 68.75%. This indicates that participants express negative or even strong aversion to these scenarios, possibly reflecting concerns about the spread, misuse, and commercialization of their information. "If the user has given consent" showed significant differences in 50% of cases, and the heatmap in Figure 5 indicates that participants are more positive about transmitting and sharing information with consent.

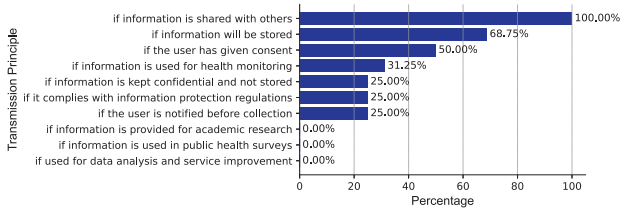


Figure 6: The percentage of instances where the inclusion of the specified transmission principle resulted in a statistically significant difference in acceptability scores compared to the same information flow with the *null* transmission principle.

Thus, we arrive at conclusions similar to those of Apthorpe et al. [42] and Kablo et al. [43], where transmission principles significantly influence how participants perceive the accessibility of LLM-based healthcare consul-

tation information. Notably, the last three principles did not yield lower or negative scores, nor did they show significant differences. This suggests that participants do not exhibit a clear preference against these conditions, possibly due to the perceived social contributions or service improvement values associated with these principles, which they feel do not overly infringe on their privacy.

4.2.3. Effect of Demographics. We conducted significance tests on groups formed under 10 demographic characteristics, with a corrected significance threshold of 0.005. Significant differences were found within 6 groups: age, education, privacy learning background, medical background, LLM knowledge, and experienced health privacy breach (see Table 4 in Appendix B).

Younger/Higher Educated Individuals Show Less Openness. Unlike CI-based privacy norm surveys in the West [43], our survey found that participants over 35 (average score of 0.65) were more willing to share LLM-based healthcare information than those under 35 (average score of 0.47), with a significant difference (p <.005). Furthermore, younger participants exhibited greater variability in acceptability scores across transmission principles, suggesting clearer privacy norms and better awareness of risks. Similarly, participants with more education or research experience assessed different information flows more critically. Overall, participants with master's degrees or higher had a significantly different average acceptability score (0.41) compared to those with other educational backgrounds (0.53) (p <.005).

Medical Background and LLM Knowledge Influence Expectations. Apart from the information flows under *null* principles, participants with a medical background had higher average scores than others in information flows with other principles. The average acceptability score for the group with a medical background was 0.68, higher than the average score of 0.47 for others, with a significant difference in acceptability between the two groups (p <.005). This distinction was particularly pronounced in the last three principles, where those with a medical background were more open to using LLM-based healthcare consultation information for academic research, public health surveys, and service improvement. This indicates they are more accepting of healthcare information being used beneficially and shared with entities that require it for legitimate purposes. Additionally, groups with LLM knowledge, who have heard of LLMs, used LLMs, or even used LLMs for healthcare consultation, have a higher average acceptability score (0.52) than those without LLM knowledge (0.39), with p <.005.

Health Privacy Breach Victims Are More Concerned, While Privacy Course Learners Are Not. Those who have experienced health privacy breaches show lower tolerance compared to those who have not, with average scores of 0.42 and 0.56 and statistically significant (p <.005). This indicates that encounters with health privacy issues make users more cautious about sharing their LLM-based healthcare consultation conversations. However, individuals who claim to have taken courses in data security and privacy have an average acceptability score of 0.55, higher than the 0.48 average score of those without a privacy learning background, with a statistically significant difference (p <.005). We will explore a similar paradox in the following analysis.

4.2.4. Self-Reports Correlates with Privacy Expectations. We conducted significance tests on groups formed under 8 different self-reported attitudes, adjusting the significance threshold to 0.00625. Specifically, for groups with unbalanced sample distributions and insufficient sample sizes for the minority class as required by power analysis, we include samples labeled "*Neutral*" in the minority class. Overall, participants' attitudes demonstrated certain privacy expectations, with significant differences found in 7 of these categorized groups (See Table 5 in Appendix B).

Attitudes Align with Expectations. Participants who reported providing basic information during the consultation showed higher acceptability for recipients accessing information, with an average score of 0.56 compared to 0.35 for those who did not provide information. This difference is statistically significant (p <.00625). On the other hand, a significant difference was observed between participants inclined to adopt the advice obtained from consultations and other participants (including *Neutral*). The former group's average acceptability score (0.58) was more than twice as high as that of the latter group (0.29). Moreover, participants who anticipated using reliable LLMs for future healthcare consultations exhibited a greater openness to information sharing, with an average acceptability score of 0.60, significantly higher than 0.17 for the remaining participants (including *Neutral*) (p <.00625). Additionally, the group that perceived no compromise to privacy in online interactions with chatbots had a higher acceptability score (average of 0.55), which is statistically different from the acceptability score of the remaining group (including *Neutral*), with an average of 0.39. Similar to the findings of Kablo et al. [43], we observed that independence in evaluating different transmission principles significantly impacts participants' acceptability scores (p <.00625). Specifically, the first group, which considered "if the user has given consent" as a precondition for evaluating subsequent transmission principles, scored an average acceptability of 0.57, higher than that of the group that assessed all information flows independently (0.35), with 629 participants (74.3%) always considering consent as a given. The above analyses indicate that participants' attitudes are linked to their privacy expectations, showing consistent trends.

Instances of Privacy Illusions. Interesting trends emerged where participants' self-reported situations created noteworthy differences in line with privacy expectations. Participants who believed they would verify the advice generated in consultations (choosing *Likely* and *Extremely likely*) **showed higher acceptability scores** across different transmission principles than those who deemed it less likely (choosing *Unlikely* and *Extremely unlikely*), with average scores of 0.60 and 0.31, respectively. This difference is statistically significant (p <.00625), indicating that verifying LLM-generated healthcare advice does not imply a more

negative expectation toward information access. Conversely, those unlikely to verify advice were less willing to share information. We refer to this paradox between self-reporting and observed privacy expectations as users' "*illusion*", suggesting a mismatch between users' attitudes and their privacy norms.

Similarly, another noteworthy finding is that groups **more knowledgeable and concerned about health privacy showed higher openness to information access**, with average acceptability scores of 0.66 and 0.48 respectively. This is higher than groups with less privacy knowledge and concern, with average scores of 0.34 and 0.12. Furthermore, a significant difference (p <.00625) was found between groups with and without health privacy knowledge. Those informed and concerned about health privacy did not exhibit a closed-off trend regarding sharing information, likely due to a clearer comprehension of its purposes, such as its inevitable use in academic research and service improvement. On the other hand, it is necessary to caution users against falling into "illusions" of believing they understand and care about health privacy, which could lead to more exposure of their information.

In fact, previous studies have found inconsistencies between what people say and their actual actions regarding privacy and security [71]–[73]. We observe that in the context of LLM-based healthcare consultations, **LLMs are likely to further exacerbate this paradox**. Although users express concerns, they often engage in potentially risky behaviors due to the overwhelming trend and curiosity surrounding LLMs.

5. Discussion and Future Work

This section discusses the phenomena and insights revealed by this study, provides challenges and suggestions for future work, and outlines the comparative novelty and limitations of this research.

5.1. Comparison of Privacy Expectations

Impact of Cultural Differences on Privacy. Our survey indicates that users' privacy expectations and norms are closely related to their personal backgrounds and experiences. Participants who are younger, more educated, and lack a medical background are less accepting of LLM-based health information transmission. These observations contrast with findings by Kablo et al. [43], who noted that younger and more educated participants were more open to sharing neurodata, caring less about sharing brain signals. This difference highlights the unique privacy norms regarding LLM-based healthcare consultations in China, where there is generally a weaker awareness and higher acceptance of information transmission [27], [29]. This underscores the necessity of conducting LLM-based healthcare privacy surveys in China and other non-Western regions with diverse backgrounds.

Impact of Principles and Research Topics. Our findings also emphasize how various information transmission principles significantly influence users' privacy expectations. Consistent with the previous research [41]–[43], principles regarding consent are crucial for enhancing the acceptability of information sharing, while sharing information with third parties or storing information is deemed unacceptable. Interestingly, due to the unique nature of the topic of LLM-based healthcare consultations, users are not overly resistant to the use of information for health monitoring, academic research, public health surveys, data analysis, and service improvement, especially when considering healthcare providers and medical information.

Acceptance of LLM-based Healthcare Consultations. Furthermore, the analysis indicates that users are willing to embrace LLM-based healthcare consultation services. Factors such as convenience, lower costs, and supplementing medical knowledge positively drive users towards LLM-based healthcare consultations, with some users also expressing trust in the LLMs to secure and protect their privacy. Focusing on general health issues could enhance user compliance, aligning with findings by Chen et al. [74], which suggest that overly personalized services could infringe on privacy, as indicated by our qualitative analysis of user feedback.

Although previous studies do not provide directly comparable quantitative analysis data, research conducted in China on digital health indicates that Chinese people have relatively weak trust in digital medical services and multifaceted privacy concerns (though not as strong as in Western countries) [27], [75]. In contrast, we observe that participants exhibit relatively low concern about the privacy risks associated with LLM-based healthcare consultations. Our analysis suggests that ***this phenomenon is likely related to the prevalence of LLMs, which has generated a strong willingness among users to engage and explore***.

5.2. Privacy Protection Challenges and Directions

5.2.1. Weaknesses in User Privacy and Protection Technologies. We observe vulnerabilities in both user privacy and privacy protection technologies. Despite less than half of the participants claiming a comprehensive understanding of health privacy, the majority are willing to use "reliable" LLM-based healthcare consultations. Most are willing to provide personal information, and many trust that LLMs will keep their information confidential. Participants did not show significant resistance to principles like health monitoring, data analysis, and service improvement. Moreover, users may be caught in ***the "illusion" of understanding and valuing health privacy while being more open in practice***, such as accepting the use of data for analysis and service improvement. In an era of rapidly emerging LLM services, this could potentially lead to more risks to users' health privacy. Particularly in China, where many third-party platforms or Mini-Programs [76] can use ChatGPT, these platforms or services may integrate private plugins from developers or collect and store user data. The severe situation presents challenges to privacy in LLM-based healthcare consultations due to users' lack of concern.

Participants' responses suggest that privacy protection technologies may fail to adequately safeguard users' health privacy from being captured by recommendation algorithms. Before recommending products and services, are these privacy protection technologies properly informing users and obtaining their consent? This "disappearance" of privacy protection technology frequently appears in previous technologies, and users are unwilling to see it happen after LLM-based healthcare consultations. However, ***the current strategies or technologies of LLMs do not provide adequate protection***. For instance, OpenAI's privacy policy [77] indicates that they may disclose personal information to their affiliates; when mentioning de-identification, they only state that they "may" take this measure. Consequently, users' health privacy is more susceptible to subsequent impacts in practice.

5.2.2. Privacy Tech Must Evolve with the LLM Era. First, ***enhancing the conveyance of privacy protections is crucial***. As consent principles significantly impact information sharing [43], [78], emphasizing privacy protection technology's presence and security before, during, and after LLM use can play a decisive role, especially in preventing users from being troubled by big data and recommendation algorithms after using LLM. Participants provided suggestions in their feedback, such as *"Displaying proof that the model will not leak privacy in a prominent place in the chat window can strengthen users' trust and encourage them to raise their issues more confidently" (P63)*. It is noteworthy that participants did not express significant concern about privacy when using LLMs for healthcare advice, with the average acceptability scores for different recipients or attributes all being greater than 0, as shown in Section 4.2.1. Since we disclosed the potential risks in the informed consent form, this phenomenon is likely because users did not thoroughly read the informed consent, particularly OpenAI's privacy policy, as they often do in practice. Hence, ***employing detection technologies to identify uninformed users and automatically convey privacy issue***s is essential [79]–[81]. For instance, context-aware technologies could be implemented in LLM-based systems to issue personalized privacy reminders based on the user's current behavior and interaction context.

Furthermore, ***enhancing data anonymity and transparency is urgent***. In recent years, attacks targeting LLMs have become increasingly prevalent, such as personal identity extraction attacks [82] and poisoning training data to reveal private information [83]. Therefore, corresponding defense measures should be iteratively updated in a timely manner. For example, researchers can employ encryption methods that allow LLMs to perform inference and respond to encrypted inputs without decrypting user data [84]. In terms of transparency, LLM service providers should offer sufficient explanatory capability for their algorithmic decision-making, including interpretable models and interface designs, enabling users to intuitively understand the source and logic behind the advice. Moreover, LLM service providers should offer users ways to query data usage and how to delete or correct their data. Combining blockchain technology can ensure the traceability and process transparency of health information in LLM consultations [85], and developing detection tools can proactively assess the risk of personal identity information leakage [86].

In addition, ***exploring interdisciplinary approaches to privacy protection is essential***. Legal, ethical, and sociopsychological factors should be considered and integrated into privacy protection technologies, helping to form more practical and human-centric protection frameworks. For instance, a balance needs to be achieved between respecting privacy and personalization. Customization that adapts to users' privacy and aesthetic preferences can offer more precise personalization and minimize user dissatisfaction [87], [88]. Lastly, considering cultural and regional differences, a new paradigm of LLM privacy protection that aligns with actual conditions should be established. We recommend promptly conducting cross-cultural and cross-regional studies on LLM health privacy awareness to verify whether existing protection methods meet the users' expectations.

5.2.3. Privacy Legislation and Regulation. As discussed in Section 4.2.1, a noteworthy observation in the survey of participants' privacy norms is that the acceptability scores for information flows under the principle of "if it complies with information protection regulations" did not show a high level, indicating a lack of confidence among users regarding these regulations. Similar to previous research [42] that revealed a general distrust among users towards dense and lengthy privacy policies [89], participants from China also did not demonstrate a high trust in privacy laws. Although the Chinese public tends to trust the government [26], [27], [29], the interest and capability in privacy regulation are limited [90], [91], with notable issues such as fragmented privacy regulations, delayed legislation, and insufficient consideration of privacy protections [92]. Consequently, it is recommended to address gaps and delays in existing legal frameworks, improve the clarity of legal provisions, specify conditions and time limits for information transmission, and implement fine-grained controls on information flow management.

5.3. Comparative Novelty and Future Research Implications

Compared to related work [11], [33], [36], our study demonstrates distinct novelty in several aspects: the **Problem**—focusing on privacy issues and unique trends in China, which prior research has not deeply explored; the **Approach**—integrating the ChatGPT interface and applying Contextual Integrity, setting it apart from traditional survey methods; and the **Results**—providing both quantitative and qualitative insights into critical risks and challenges for future technological development regarding this important yet underexplored problem.

In light of the insights gained from this user study, future research in this direction should emphasize comparing the study contexts, applied methods, and derived conclusions. It

is recommended to focus on different cultural backgrounds, enrich CI parameters with finer granularity, explore diverse underlying LLMs, optimize chatbot interactions and interface design, and investigate real-world applications of LLM-based healthcare consultation services.

5.4. Limitations

Method. Similar to other survey-based studies, our research is subject to the limitations of self-reporting. Individual reports of privacy attitudes may be higher than actual behaviors reveal [93], [94]. To mitigate this, we designed an online chatbot for users to interact with, collecting their first feedback and observing it. Nevertheless, the interface interaction and response quality might have influenced participants' perceptions. We took measures to alleviate these impacts, including providing reminders, a range of options, and free-text descriptions for participants.

Sample. Typical of crowd-sourced research, our sample is biased towards younger, more educated demographics [95]. All participants are from China, and cultural differences mean these results cannot be generalized to other countries. Although our participants cover all provinces of Mainland China and are quite diverse, they still do not fully represent the Chinese population. We do not attempt to generalize our findings but seek insightful perceptions through quantitative and qualitative analyses. Future research could validate our findings and consider a global perspective, extending them to a broader range of participants.

Scope. Our study focuses on privacy issues by investigating user awareness and expectations in LLM-based healthcare consultations. To gain more comprehensive and profound perspectives, it is necessary to conduct in-depth interviews with users from diverse backgrounds. Additionally, future research could involve longitudinal measurements to discover whether privacy norms yield the anticipated effects over time.

6. Conclusion

In this paper, we pave a new avenue to understand users' privacy awareness and expectations regarding emerging LLM-based healthcare consultations. To achieve this goal, we first design an LLM-based healthcare chatbot to observe users' privacy awareness during usage. Moreover, we test the acceptability of consultation information flows based on the theory of contextual integrity. Our analysis of the collected responses reveals that Chinese users' trust and acceptance of LLM-based healthcare consultants outweigh their privacy concerns. Their privacy expectations are primarily associated with information transmission principles, demographics, and self-reported attitudes, encompassing some contradictory trends. We believe our work lays the foundation for exploring privacy practices in LLM-based healthcare applications and advancing its privacy protection methods.

Acknowledgments

We thank the reviewers for their valuable feedback. This work was supported in part by the National Key Research and Development Program of China under Grant 2022YFF1203001; in part by the National Natural Science Foundation of China under Grants 62172155, 62072465, 62102425, 62472434, U22B2005; and in part by the Science and Technology Innovation Program of Hunan Province under Grant 2022RC3061.

References

[1] K. Singhal, S. Azizi, T. Tu, S. S. Mahdavi, J. Wei *et al.*, "Large language models encode clinical knowledge," *Nature*, vol. 620, no. 7972, pp. 172–180, 2023.

[2] A. J. Thirunavukarasu, D. S. J. Ting, K. Elangovan, L. Gutierrez, T. F. Tan, and D. S. W. Ting, "Large language models in medicine," *Nature Medicine*, vol. 29, no. 8, pp. 1930–1940, 2023.

[3] Z. Kanjee, B. Crowe, and A. Rodman, "Accuracy of a generative artificial intelligence model in a complex diagnostic challenge," *JAMA*, vol. 330, no. 1, pp. 78–80, 2023.

[4] B. Huo, G. E. Cacciamani, G. S. Collins, T. McKechnie, Y. Lee, and G. Guyatt, "Reporting standards for the use of large language model-linked chatbots for health advice," *Nature Medicine*, vol. 29, no. 12, pp. 2988–2988, 2023.

[5] N. Saif, S. U. Khan, I. Shaheen, A. ALotaibi, M. M. Alnfiai, and M. Arif, "Chat-gpt; validating technology acceptance model (tam) in education sector via ubiquitous learning mechanism," *Computers in Human Behavior*, vol. 154, p. 108097, 2024.

[6] P. Webster, "Six ways large language models are changing healthcare," *Nature Medicine*, vol. 29, no. 12, pp. 2969–2971, 2023.

[7] "Chatgpt diagnoses 4 yr olds chronic pain after 17 doctors fail to do so," https://economictimes.indiatimes.com/news/new-updates/chatgpt-diagnoses-4-yr-olds-chronic-pain-after-17-doctors-fail-to-do-so/articleshow/103622026.cms?from=mdr, 2023.

[8] G. Times, "Top 10 chinese buzzwords of 2023 released - global times," https://www.globaltimes.cn/page/202312/1303082.shtml, 2023.

[9] "Baidu says ai chatbot 'ernie bot' has attracted 200 million users," https://www.reuters.com/technology/baidu-says-ai-chatbot-ernie-bot-has-amassed-200-million-users-2024-04-16/, 2024.

[10] K. Connection, "iflytek's spark cognitive model: A beacon or a mirage in the ai landscape?" https://kr-asia.com/iflyteks-spark-cognitive-model-a-beacon-or-a-mirage-in-the-ai-landscape, 2023.

[11] Y. Xiao, K. Z. Zhou, Y. Liang, and K. Shu, "Understanding the concerns and choices of public when using large language models for healthcare," *arXiv preprint arXiv:2401.09090*, 2024.

[12] "China's internet medical service users hit 363 mln: Report - people's daily online," http://en.people.cn/n3/2023/0303/c90000-10215542.html, 2023.

[13] "Digital health - china," https://www.statista.com/outlook/hmo/digital-health/china, 2024, accessed on: 2024-06-03.

[14] Anubhav, "Tencent's big move into ai-enhanced healthcare in china," https://www.gizmochina.com/2023/11/22/tencent-ai-healthcare-china/, 2023.

[15] "China: Size of the large medical ai model market 2023-2030," https://www.statista.com/statistics/1441186/china-size-of-the-large-medical-ai-model-market/, 2024, accessed on: 2024-06-03.

[16] H.-P. H. Lee, Y.-J. Yang, T. S. Von Davier, J. Forlizzi, and S. Das, "Deepfakes, phrenology, surveillance, and more! a taxonomy of ai privacy risks," in *Proceedings of the CHI Conference on Human Factors in Computing Systems*, 2024, pp. 1–19.

[17] B. Edwards, "Artist finds private medical record photos in popular ai training data set," https://arstechnica.com/information-technology/2022/09/artist-finds-private-medical-record-photos-in-popular-ai-training-data-set/, 2022.

[18] C. Wang, S. Liu, H. Yang, J. Guo, Y. Wu, and J. Liu, "Ethical considerations of using chatgpt in health care," *Journal of Medical Internet Research*, vol. 25, no. 1, p. e48009, 2023.

[19] "Chatgpt leaks sensitive data - spiceworks," https://www.spiceworks.com/tech/artificial-intelligence/news/chatgpt-leaks-sensitive-user-data-openai-suspects-hack/, 2024.

[20] C. E. Haupt and M. Marks, "Ai-generated medical advice—gpt and beyond," *JAMA*, vol. 329, no. 16, pp. 1349–1350, 2023.

[21] W. M. Si, M. Backes, J. Blackburn, E. De Cristofaro, G. Stringhini, S. Zannettou, and Y. Zhang, "Why so toxic? measuring and triggering toxic behavior in open-domain chatbots," in *Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security*, 2022, pp. 2659–2673.

[22] C. Peng, X. Yang, A. Chen, K. E. Smith, N. PourNejatian, A. B. Costa, C. Martin, M. G. Flores, Y. Zhang, T. Magoc, G. Lipori, D. A. Mitchell, N. S. Ospina, M. M. Ahmed, W. R. Hogan, E. A. Shenkman, Y. Guo, J. Bian, and Y. Wu, "A study of generative large language model for medical research and healthcare," *npj Digital Medicine*, vol. 6, no. 1, pp. 1–10, 2023.

[23] MAGGIE. HARRISON, "Startup shocked when 4chan immediately abuses its voice-cloning ai," https://futurism.com/startup-4chan-voice-cloning-ai, 2023.

[24] S. Magazine and E. Feldman, "Are a.i. image generators violating copyright laws?" https://www.smithsonianmag.com/smart-news/are-ai-image-generators-stealing-from-artists-180981488/, 2023.

[25] L. Giannotti, "The state of ai regulation around the world," https://www.techmonitor.ai/digital-economy/ai-and-automation/the-state-of-ai-regulation-around-the-world, 2024.

[26] F. Feng, X. Wang, and T. Chen, "Analysis of the attributes of rights to inferred information and china's choice of legal regulation," *Computer Law & Security Review*, vol. 41, p. 105565, 2021.

[27] G. Huang, A. Hu, and W. Chen, "Privacy at risk? understanding the perceived privacy protection of health code apps in china," *Big Data & Society*, vol. 9, no. 2, p. 20539517221135132, 2022.

[28] Y. Wang, H. Xia, and Y. Huang, "Examining american and chinese internet users' contextual privacy preferences of behavioral advertising," in *Proceedings of the 19th ACM Conference on Computer-Supported Cooperative Work & Social Computing*, 2016, pp. 539–552.

[29] C. Utz, S. Becker, T. Schnitzler, F. M. Farke, F. Herbert, L. Schaewitz, M. Degeling, and M. Dürmuth, "Apps against the spread: Privacy implications and user acceptance of covid-19-related smartphone apps on three continents," in *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, 2021, pp. 1–22.

[30] S. Lim and R. Schmälzle, "Artificial intelligence for health message generation: An empirical study using a large language model (llm) and prompt engineering," *Frontiers in Communication*, vol. 8, 2023.

[31] T. I. Wilhelm, J. Roos, and R. Kaczmarczyk, "Large language models for therapy recommendations across 3 clinical specialties: Comparative study," *Journal of Medical Internet Research*, vol. 25, p. e49324, 2023.

[32] R. S. Huang, K. J. Q. Lu, C. Meaney, J. Kemppainen, A. Punnett, and F.-H. Leung, "Assessment of resident and ai chatbot performance on the university of toronto family medicine residency progress test: Comparative study," *JMIR Medical Education*, vol. 9, no. 1, p. e50514, 2023.

[33] A. Choudhury, S. Elkefi, and A. Tounsi, "Exploring factors influencing user perspective of chatgpt as a technology that assists in healthcare decision making: A cross sectional survey study," *PLoS One*, vol. 19, no. 3, p. e0296151, 2024.

[34] O. Nov, N. Singh, and D. Mann, "Putting chatgpt's medical advice to the (turing) test: Survey study," *JMIR Medical Education*, vol. 9, no. 1, p. e46939, 2023.

[35] C.-H. Chuan, W.-H. S. Tsai, D. Lun, and N. Carcioppolo, "Understanding responses to embarrassing questions in chatbot-facilitated medical interview conversations using deep language models," in *Future Research Directions in Computational Intelligence*, 2024, pp. 17–25.

[36] A. Raina, P. Mishra, H. goyal, and D. Kumar, "AI as a medical ally: Evaluating chatgpt's usage and impact in indian healthcare," *arXiv preprint arXiv:2401.15605*, 2024.

[37] E. Jo, D. A. Epstein, H. Jung, and Y.-H. Kim, "Understanding the benefits and challenges of deploying conversational ai leveraging large language models for public health intervention," in *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*, 2023, pp. 1–16.

[38] Z. Yang, X. Xu, B. Yao, S. Zhang, E. Rogers, S. Intille, N. Shara, G. G. Gao, and D. Wang, "Talk2care: Facilitating asynchronous patient-provider communication with large-language-model," *arXiv preprint arXiv:2309.09357*, 2023.

[39] N. Gerber, P. Gerber, and M. Volkamer, "Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behavior," *Computers & Security*, vol. 77, pp. 226–261, 2018.

[40] J. Colnago, L. F. Cranor, A. Acquisti, and K. H. Stanton, "Is it a concern or a preference? an investigation into the ability of privacy scales to capture and distinguish granular privacy constructs," in *Eighteenth Symposium on Usable Privacy and Security (SOUPS 2022)*, 2022, pp. 331–346.

[41] N. Apthorpe, Y. Shvartzshnaider, A. Mathur, D. Reisman, and N. Feamster, "Discovering smart home internet of things privacy norms using contextual integrity," *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, vol. 2, no. 2, pp. 59:1–59:23, 2018.

[42] N. Apthorpe, S. Varghese, and N. Feamster, "Evaluating the contextual integrity of privacy regulation: Parents' IoT toy privacy norms versus COPPA," in *28th USENIX Security Symposium (USENIX Security 19)*, 2019, pp. 123–140.

[43] E. Kablo and P. Arias-Cabarcos, "Privacy in the age of neurotechnology: Investigating public attitudes towards brain data collection and use," in *Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security*, 2023, pp. 225–238.

[44] M. Minaei, M. Mondal, and A. Kate, "Empirical understanding of deletion privacy: Experiences, expectations, and measures," in *31st USENIX Security Symposium (USENIX Security 22)*, 2022, pp. 3415–3432.

[45] H. Nissenbaum, "Privacy as contextual integrity," *Washington Law Review*, vol. 79, p. 119, 2004.

[46] P. Shi, H. Xu, and Y. Chen, "Using contextual integrity to examine interpersonal information boundary on social network sites," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 2013, pp. 35–38.

[47] Y. Shvartzshnaider, S. Tong, T. Wies, P. Kift, H. Nissenbaum, L. Subramanian, and P. Mittal, "Learning privacy expectations by crowdsourcing contextual informational norms," *Proceedings of the AAAI Conference on Human Computation and Crowdsourcing*, vol. 4, pp. 209–218, 2016.

[48] Y. Shvartzshnaider, N. Apthorpe, N. Feamster, and H. Nissenbaum, "Going against the (appropriate) flow: A contextual integrity approach to privacy policy analysis," *Proceedings of the AAAI Conference on Human Computation and Crowdsourcing*, vol. 7, pp. 162–170, 2019.

[49] L. Geierhaas, F. Otto, M. Häring, and M. Smith, "Attitudes towards client-side scanning for csam, terrorism, drug trafficking, drug use and tax evasion in germany," in *2023 IEEE Symposium on Security and Privacy (SP)*, 2023, pp. 217–233.

[50] R. Cummings, G. Kaptchuk, and E. M. Redmiles, ""I need a better description": An investigation into user expectations for differential privacy," in *Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security*, 2021, pp. 3037–3052.

[51] S. Manandhar, K. Singh, and A. Nadkarni, "Towards automated regulation analysis for effective privacy compliance," in *Proceedings 2024 Network and Distributed System Security Symposium*, 2024.

[52] Z. Zhang, M. Jia, H.-P. H. Lee, B. Yao, S. Das, A. Lerner, D. Wang, and T. Li, ""It's a fair game", or is it? examining how users navigate disclosure risks and benefits when using llm-based conversational agents," in *Proceedings of the CHI Conference on Human Factors in Computing Systems*, 2024, pp. 1–26.

[53] D. Kekulluoglu and Y. Acar, ""We are a startup to the core": A qualitative interview study on the security and privacy development practices in turkish software startups," in *2023 IEEE Symposium on Security and Privacy (SP)*, 2022, pp. 2015–2031.

[54] M. Mustafa, A. M. Asad, S. Hassan, U. Haider, Z. Durrani, and K. Krombholz, "Pakistani teens and privacy - how gender disparities, religion and family values impact the privacy design space," in *Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security*, 2023, pp. 195–209.

[55] P. Liu, S. Ji, L. Fu, K. Lu, X. Zhang, J. Qin, W. Wang, and W. Chen, "How iot re-using threatens your sensitive data: Exploring the user-data disposal in used iot devices," in *2023 IEEE Symposium on Security and Privacy (SP)*, 2023, pp. 3365–3381.

[56] Y. Chen, M. Zha, N. Zhang, D. Xu, Q. Zhao, X. Feng, K. Yuan, F. Suya, Y. Tian, K. Chen, X. Wang, and W. Zou, "Demystifying hidden privacy settings in mobile apps," in *2019 IEEE Symposium on Security and Privacy (SP)*, 2019, pp. 570–586.

[57] Y. Feng, R. Zhai, R. Sion, and B. Carbunar, "A study of china's censorship and its evasion through the lens of online gaming," in *32nd USENIX Security Symposium (USENIX Security 23)*, 2023, pp. 2599–2616.

[58] "Personal information protection law of the people's republic of china," *Wikipedia*, 2024.

[59] V. Distler, M. Fassl, H. Habib, K. Krombholz, G. Lenzini, C. Lallemand, L. F. Cranor, and V. Koenig, "A systematic literature review of empirical methods and risk representation in usable privacy and security research," *ACM Transactions on Computer-Human Interaction*, vol. 28, no. 6, pp. 43:1–43:50, 2021.

[60] w. kuo, "China market research tool," https://williamkuo1988.medium.com/china-market-research-tool-e612d559b649, 2018.

[61] M. Wei, P. Emami-Naeini, F. Roesner, and T. Kohno, "Skilled or gullible? gender stereotypes related to computer security and privacy," in *2023 IEEE Symposium on Security and Privacy (SP)*, 2022, pp. 2050–2067.

[62] W. Yaqub, O. Kakhidze, M. L. Brockman, N. Memon, and S. Patil, "Effects of credibility indicators on social media news sharing intent," in *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, 2020, pp. 1–14.

[63] J. Mink, L. Luo, N. M. Barbosa, O. Figueira, Y. Wang, and G. Wang, "DeepPhish: Understanding user trust towards artificially generated profiles in online social networks," in *31st USENIX Security Symposium (USENIX Security 22)*, 2022, pp. 1669–1686.

[64] X. Huang, Y. Shi, H. Yao, M. Li, Z. Lei, J. Shi, B. Li, W. Zhang, and W. Jian, "Weight loss using an mhealth app among individuals with obesity in different economic regions of china: Cohort study," *JMIR mHealth and uHealth*, vol. 12, no. 1, p. e48675, 2024.

[65] K. Spiel, O. L. Haimson, and D. Lottridge, "How to do better with gender on surveys: a guide for hci researchers," *interactions*, vol. 26, no. 4, pp. 62–65, 2019.

[66] R. E. Boyatzis, *Transforming Qualitative Information: Thematic Analysis and Code Development*. Sage, 1998.

[67] M. B. Miles and A. M. Huberman, *Qualitative Data Analysis: An Expanded Sourcebook*. Sage, 1994.

[68] G. Petracca, A.-A. Reineh, Y. Sun, J. Grossklags, and T. Jaeger, "AWare: Preventing abuse of Privacy-Sensitive sensors via operation bindings," in *26th USENIX Security Symposium (USENIX Security 17)*, 2017, pp. 379–396.

[69] E. Toch, Y. Wang, and L. F. Cranor, "Personalization and privacy: A survey of privacy risks and remedies in personalization-based systems," *User Modeling and User-Adapted Interaction*, vol. 22, no. 1, pp. 203–220, 2012.

[70] A. Choudhury and H. Shamszare, "Investigating the impact of user trust on the adoption and use of chatgpt: Survey analysis," *Journal of Medical Internet Research*, vol. 25, no. 1, p. e47184, 2023.

[71] J. Gideon, L. Cranor, S. Egelman, and A. Acquisti, "Power strips, prophylactics, and privacy, oh my!" in *Proceedings of the Second Symposium on Usable Privacy and Security*, 2006, pp. 133–144.

[72] S. Egelman, J. King, R. C. Miller, N. Ragouzis, and E. Shehan, "Security user studies: Methodologies and best practices," in *CHI '07 Extended Abstracts on Human Factors in Computing Systems*, 2007, pp. 2833–2836.

[73] A. Sotirakopoulos, K. Hawkey, and K. Beznosov, "On the challenges in usable security lab studies: Lessons learned from replicating a study on ssl warnings," in *Proceedings of the Seventh Symposium on Usable Privacy and Security*, 2011, pp. 1–18.

[74] J. Chen, C. Chen, J. B. Walther, and S. S. Sundar, "Do you feel special when an ai doctor remembers you? individuation effects of ai vs. human doctors on user experience," in *Extended Abstracts of the 2021 CHI Conference on Human Factors in Computing Systems*, 2021, pp. 1–7.

[75] L. Sun, "Health data governance in china: Emphasizing 'sharing' and 'protection' based on the right to health," *Medical Law International*, vol. 23, no. 1, pp. 26–43, 2023.

[76] "What are wechat mini-programs? a simple introduction," https://walkthechat.com/wechat-mini-programs-simple-introduction/, 2019.

[77] "Privacy policy," https://openai.com/policies/privacy-policy/, 2023.

[78] B. Kacsmar, K. Tilbury, M. Mazmudar, and F. Kerschbaum, "Caring about sharing: User perceptions of multiparty data sharing," in *31st USENIX Security Symposium (USENIX Security 22)*, 2022, pp. 899–916.

[79] T. Zheng, T. Zhou, Q. Liu, K. Wu, and Z. Cai, "Characterizing and detecting non-consensual photo sharing on social networks," in *Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security*, 2022, pp. 3209–3222.

[80] D. Franzen, S. Nuñez von Voigt, P. Sörries, F. Tschorsch, and C. Müller-Birn, "Am i private and if so, how many? communicating privacy guarantees of differential privacy with risk communication formats," in *Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security*, 2022, pp. 1125–1139.

[81] B. Kacsmar, V. Duddu, K. Tilbury, B. Ur, and F. Kerschbaum, "Comprehension from chaos: Towards informed consent for private computation," in *Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security*, 2023, pp. 210–224.

[82] N. Lukas, A. Salem, R. Sim, S. Tople, L. Wutschitz, and S. Zanella-Béguelin, "Analyzing leakage of personally identifiable information in language models," in *2023 IEEE Symposium on Security and Privacy (SP)*, 2023, pp. 346–363.

[83] F. Tramèr, R. Shokri, A. San Joaquin, H. Le, M. Jagielski, S. Hong, and N. Carlini, "Truth serum: Poisoning machine learning models to reveal their secrets," in *Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security*, 2022, pp. 2779–2792.

[84] A. Mishra, M. Li, and S. Deo, "Sentinellms: Encrypted input adaptation and fine-tuning of language models for private and secure inference," *Proceedings of the AAAI Conference on Artificial Intelligence*, vol. 38, no. 19, pp. 21 403–21 411, 2024.

[85] Z. Liu, L. Hu, Z. Cai, X. Liu, and Y. Liu, "Secose: Toward searchable and communicable healthcare service seeking in flexible and secure ehr sharing," *IEEE Transactions on Information Forensics and Security*, vol. 19, pp. 4999–5014, 2024.

[86] S. Kim, S. Yun, H. Lee, M. Gubri, S. Yoon, and S. J. Oh, "Propile: Probing privacy leakage in large language models," *Advances in Neural Information Processing Systems*, vol. 36, pp. 20 750–20 762, 2023.

[87] T. Zhou, Z. Cai, F. Liu, and J. Su, "In pursuit of beauty: Aesthetic-aware and context-adaptive photo selection in crowdsensing," *IEEE Transactions on Knowledge and Data Engineering*, vol. 35, no. 9, pp. 9364–9377, 2023.

[88] Y. Feng, Y. Yao, and N. Sadeh, "A design space for privacy choices: Towards meaningful privacy control in the internet of things," in *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, 2021, pp. 1–16.

[89] B. Chen, T. Wu, Y. Zhang, M. B. Chhetri, and G. Bai, "Investigating users' understanding of privacy policies of virtual personal assistant applications," in *Proceedings of the 2023 ACM Asia Conference on Computer and Communications Security*, 2023, pp. 65–79.

[90] A. Lv and T. Luo, "Asymmetrical power between internet giants and users in china," *International Journal of Communication*, vol. 12, pp. 3877–3895, 2018.

[91] T. Luo and A. Lv, ""Nine dragons run the water": Fragmented internet governance in china," in *Power and Authority in Internet Governance*, 2021.

[92] Y. Xiao, "Research on legal constraints of individual environmental data rights and interests in big data environment," *Journal of Environmental and Public Health*, vol. 2022, pp. 1–11, 2022.

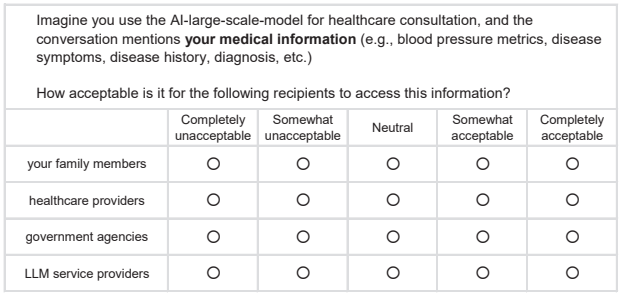
[93] A. Acquisti, L. Brandimarte, and G. Loewenstein, "Privacy and human behavior in the age of information," *Science*, vol. 347, no. 6221, pp. 509–514, 2015.

[94] S. Kokolakis, "Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon," *Computers & Security*, vol. 64, pp. 122–134, 2017.

[95] E. M. Redmiles, S. Kross, and M. L. Mazurek, "How well do my results generalize? comparing security and privacy survey results from mturk, web, and telephone samples," in *2019 IEEE Symposium on Security and Privacy (SP)*, 2019, pp. 1326–1343.

Appendix A. Survey Instrument

To enhance detail and reproducibility, we provide the prototype system code, redacted datasets, and statistical analysis scripts without raising ethical concerns. Further resources can be found at https://anonymous.4open.science/r/LLMHealthPrivacy_UserStudy-F25F. The deployed system is available at http://healthllm.top/LLMHPri/encindexzh/ (the English version is available at http://healthllm.top/LLMHPri/encindexen/). For ethical considerations, we have disabled the website link distributed to participants and replaced it with the above link. The now available link removes some of the *Quality Control* methods such as restricting repeat participation in the survey. The system includes the informed consent form, the healthcare chatbot interface, and the embedded questionnaire. A complete

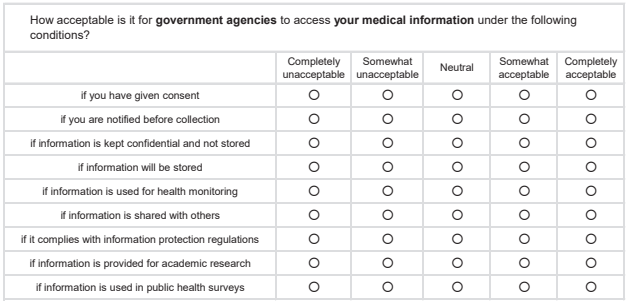


Imagine you use the AI-large-scale-model for healthcare consultation, and the conversation mentions **your medical information** (e.g., blood pressure metrics, disease symptoms, disease history, diagnosis, etc.)

How acceptable is it for the following recipients to access this information?

	Completely unacceptable	Somewhat unacceptable	Neutral	Somewhat acceptable	Completely acceptable
your family members	○	○	○	○	○
healthcare providers	○	○	○	○	○
government agencies	○	○	○	○	○
LLM service providers	○	○	○	○	○

Figure 7: Example matrix-like block shown to participants for the acceptability of *medical information* accessed by different recipients (*null* principle).



How acceptable is it for **government agencies** to access **your medical information** under the following conditions?

	Completely unacceptable	Somewhat unacceptable	Neutral	Somewhat acceptable	Completely acceptable
if you have given consent	○	○	○	○	○
if you are notified before collection	○	○	○	○	○
if information is kept confidential and not stored	○	○	○	○	○
if information will be stored	○	○	○	○	○
if information is used for health monitoring	○	○	○	○	○
if information is shared with others	○	○	○	○	○
if it complies with information protection regulations	○	○	○	○	○
if information is provided for academic research	○	○	○	○	○
if information is used in public health surveys	○	○	○	○	○

Figure 8: Example matrix-like block shown to participants for the acceptability of *government agencies* accessing *medical information* under different transmission principles.

questionnaire sample can be found at https://www.wjx.cn/vm/rQgVlKX.aspx#. Due to space constraints, only details related to RQ2 are provided here, starting with Q8 of the questionnaire.

Privacy Expectations (RQ2)

In this part, each participant is randomly assigned two blocks with the same *ATTRIBUTE*, one containing *null* transmission principle information flows with different *recipients* (i.e., Q8. An example is shown in Figure 7), and the other containing information flows with *different transmission principles* but the same *RECIPIENT* (i.e., Q9. An example is shown in Figure 8).

Q8 Imagine you use the AI-large-scale-model for healthcare consultation, and the conversation mentions your *[ATTRIBUTE]* (e.g., *[illustrate with examples]*.) How acceptable is it for the following recipients to access this information?
(Answer choices: ○ Completely unacceptable ○ Somewhat unacceptable ○ Neutral ○ Somewhat acceptable ○ Completely acceptable)

Q8.1 Your family members
Q8.2 Healthcare providers
Q8.3 Government agencies
Q8.4 LLM service providers

Q9 How acceptable is it for *[RECIPIENT]* to access your *[ATTRIBUTE]* under the following conditions?
(Answer choices: ○ Completely unacceptable ○ Somewhat unacceptable ○ Neutral ○ Somewhat acceptable ○ Completely acceptable)

Q9.1 If you have given consent.
Q9.2 If you are notified before collection.
Q9.3 If information is kept confidential and not stored.
Q9.4 If information will be stored.

Q9.5 If information is used for health monitoring.
Q9.6 If information is shared with others.
Q9.7 If it complies with information protection regulations.
Q9.8 If information is provided for academic research.
Q9.9 If information is used in public health surveys.

Q10 Did you select the answer for each row based on "with your consent"? *For example, selecting "If information is shared with others" means "If you have given consent and information is shared with others"?* (○ Yes, I consider all scenarios with consent already in place ○ No, I did not consider the subsequent scenarios as based on consent ○ I don't know or prefer not to say)

Q11 Which option is not mentioned above? (○ You are notified before collection ○ The kind of tea you want to drink today ○ Information will be stored ○ It complies with information protection regulations)

Appendix B. Analysis Materials

The detailed demographics and technology knowledge of our participants are presented in Table 3. The 10 different demographic groups and the corresponding significance test results are shown in Table 4. The 8 different self-reported attitude groups and the corresponding significance test results are shown in Table 5.

TABLE 3: Detailed demographics and technology knowledge of survey participants (n=846).

Item	Sample (%)
Gender	
Female	419 (50%)
Male	411 (49%)
Other or prefer not to say	16 (1%)
Age	
18-24	310 (37%)
25-34	357 (42%)
35-44	105 (12%)
45-54	44 (5%)
55+	10 (1%)
Prefer not to say	20 (2%)
Education	
Less than high school	18 (2%)
High school degree	38 (5%)
Junior college	86 (10%)
Undergraduate	152 (18%)
Bachelor's degree	374 (44%)
Master's degree	126 (15%)
Doctor's degree	37 (4%)
Other or prefer not to say	15 (2%)
Area	
Eastern region	443 (52%)
Central region	194 (23%)
Western region	134 (16%)
Northeast region	78 (9%)
IT Background	
Yes	458 (54%)
No	377 (45%)
Prefer not to say	11 (1%)
Privacy Learning Background	
Yes	363 (43%)
No	461 (55%)
Prefer not to say	22 (2%)
Medical Background	
Yes	132 (16%)
No	714 (84%)
Practitioner Available for Consultation	
Yes	182 (22%)
No	641 (76%)
Prefer not to say	23 (2%)

TABLE 4: Significance test results for groups formed under 10 demographic characteristics. p-values below the adjusted 0.005 threshold are highlighted in dark red, indicating significant differences in acceptability scores between two subgroups under the specified grouping criteria.

Compared Groups	p-values & Average Acceptability Scores
Age	p=1.27e-04
18-34	0.47
35+	0.65
Gender	p=.43
Female	0.52
Male	0.50
Education	p=1.91e-03
Without higher academic degree	0.53
Master's degree and above	0.41
IT Background	p=.82
Yes	0.498
No	0.50
Privacy Learning Background	p=9.29e-04
Yes	0.55
No	0.48
Medical Background	p=3.33e-07
Yes	0.68
No	0.47
Practitioner Available for Consultation	p=.017
Yes	0.55
No	0.49
LLM Knowledge	p=1.05e-03
Yes	0.52
No	0.39
Online Healthcare Consultation Experience	p=6.27e-03
Yes	0.53
No	0.46
Experienced Health Privacy Breach	p=3.00e-06
Yes	0.42
No	0.56

TABLE 5: Significance test results for groups formed under 8 different self-reported attitudes. p-values below the adjusted 0.00625 threshold are highlighted in dark red, indicating significant differences in acceptability scores between two subgroups under the specified grouping criteria.

Compared Groups	p-values & Average Acceptability Scores
Providing Basic Information	p=2.67e-11
Yes	0.56
No	0.35
Will Verify the Generated Advice	p=8.40e-11
Yes	0.60
No	0.31
Will Adopt the Generated Advice	p=8.74e-17
Yes	0.58
No (Including *Neutral*)	0.29
Online Experience Compromises Privacy	p=2.70e-09
Yes (Including *Neutral*)	0.39
No	0.55
Will Use LLM-based Healthcare Consultation Services	p=1.87e-21
Yes	0.60
No (Including *Neutral*)	0.17
Understanding Health Privacy	p=1.10e-13
Yes	0.66
No	0.34
Concern About Health Privacy	p=.13
Yes	0.50
No (Including *Neutral*)	0.43
Assuming Consent as a Prerequisite	p=2.31e-09
Yes	0.57
No	0.35

Appendix C.
Meta-Review

The following meta-review was prepared by the program committee for the 2025 IEEE Symposium on Security and Privacy (S&P) as part of the review process as detailed in the call for papers.

C.1. Summary

This study explores Chinese users' privacy concerns and expectations when using large language models (LLMs) for healthcare consultations. Through a large-scale survey involving 846 participants, the research evaluates privacy norms based on Nissenbaum's Contextual Integrity framework, focusing on factors like recipient, transmission principles, and demographic differences. While most participants expressed privacy concerns, many were still willing to use LLMs for medical advice. However, the sharing and storage of personal information were the most unacceptable to participants. The study highlights the contradictions between privacy awareness and behavior and offers insights into the challenges of balancing privacy with the convenience of LLMs in healthcare.

C.2. Scientific Contributions

- Independent Confirmation of Important Results with Limited Prior Research
- Provides a Valuable Step Forward in an Established Field

C.3. Reasons for Acceptance

1) The paper focuses on an important and timely problem and presents comprehensive findings regarding privacy issues with LLM-based healthcare consultations.
2) The paper uses the contextual integrity framework for measuring the appropriateness of the data flows and the qualitative and quantitative methods used in the study are sound.
3) The methodology and results are well-presented and easy to understand.