Privacy Policy Evaluation and Empirical Study of Mobile Health Applications: Postprint

Authors: Ma Chengyu, Liu Qiankun

Date: 2023-04-01T16:15:52+00:00

Abstract

[Purpose/Significance] This study analyzes the current status of privacy policies of mainstream Chinese mobile health applications and proposes recommendations for improving the privacy protection mechanisms for mobile health applications in China.

[Methods/Process] Through a three-round screening process, the privacy policy texts of 104 mobile health applications were selected as research objects. The textual content was analyzed using content analysis methodology, and a comprehensive evaluation index system was constructed to systematically assess the privacy policy content.

[Results/Conclusions] The overall evaluation scores for mobile health application privacy policies are relatively low, with an average score of 44.58 out of 100. The privacy policies require improvement in both standardization and completeness, and some applications exhibit excessive collection and misuse of user privacy data. Policy recommendations are proposed from three aspects: optimizing privacy policy design, standardizing evaluation and regulatory mechanisms, and improving the legal environment for protecting users' health privacy information.

Full Text

Preamble

Volume 64, Issue 7, April 2020

Research on the Evaluation and Empirical Study of Privacy Policies for Mobile Health Applications*

Ma Chengyu, Liu Qiankun
Department of Health Management and Policy, School of Public Health, Capital Medical University, Beijing 100069

Abstract:
[**Purpose/Significance**] This study analyzes the current state of privacy policies among mainstream Chinese mobile health applications and proposes recommendations for improving China's mobile health application privacy protection mechanisms. [**Method/Process**] Through three rounds of screening, privacy policy texts from 104 mobile health applications were selected as research subjects. Content analysis was employed to examine the texts, and a comprehensive evaluation index system was constructed to systematically assess the privacy policy content. [**Result/Conclusion**] The overall evaluation score of mobile health application privacy policies was not high, with an average score of 44.58 out of 100. Privacy policies need improvement in both standardization and completeness, and some applications exhibit excessive collection and misuse of user privacy data. Policy recommendations are proposed from three aspects: optimizing privacy policy design, standardizing evaluation and regulatory mechanisms, and improving the legal environment for protecting user health privacy information.

Keywords: privacy policy; mobile health; privacy protection; regulatory mechanism
Classification Number: G25
DOI: 10.13266/j.issn.0252-3116.2020.07.006

"Internet + Healthcare" represents a new medical service model that relies on next-generation information technology to provide various applications including health management, medical consultation, appointment registration, and medication services [1]. In recent years, driven by the Healthy China and "Internet +" strategies, "Internet + Healthcare" has experienced rapid development in China. With the widespread adoption of smartphones, mobile health applications (hereinafter referred to as mobile health APPs) are widely used, creating increasing opportunities for users to disclose personal health privacy information on mobile devices. While this facilitates access to high-quality, personalized medical and health services, it also introduces significant information security risks. To address this, in December 2017, the Standardization Administration of China issued the "Information Security Technology - Personal Information Security Specification" (GB/T 35273-2017, hereinafter referred to as the "Specification"), which clarifies norms for personal information controllers regarding information collection, storage, use, sharing, transfer, and disclosure, while also providing templates to guide mobile health APPs in improving privacy protection policies. However, the effectiveness of current implementation remains lacking in quantitative evaluation. This study analyzes the current practice of privacy policies among mainstream mobile health APPs in China, identifies existing problems, and proposes countermeasures and recommendations to provide a basis for improving the privacy and security protection mechanisms of mobile health APPs.

1. Evaluation of Privacy Policies for Mobile Health Platforms at Home and Abroad

While mobile APPs provide various convenient services to smartphone users in daily life, they also record and transmit large amounts of personal information. The frequent use of mobile APPs and the extensive exchange and dissemination of information have drawn considerable attention to privacy and security issues. Currently, two primary models exist internationally for protecting personal privacy information in mobile APPs: the legislative model represented by the European Union and the corporate self-regulation model represented by the United States [2]. China adopts a model primarily based on software operator self-discipline with supplementary government supervision, where relevant government departments issue regulations and norms, and software operators independently formulate privacy protection policies to explicitly state rights, obligations, and responsibilities related to user privacy and security protection [3]. Consequently, privacy protection policies have become a crucial link in the privacy protection security chain of mobile APPs, helping users understand what information about themselves will be collected, how and why it will be collected, how it will be stored and used, and what measures will be taken for handling and remediation after information security incidents [4]. However, according to a 2018 survey report by the China Consumers Association on 100 types of APPs, nearly 34% of APPs did not publish personal privacy protection terms to users, and 41% failed to display privacy policies in prominent locations. In terms of readability of self-regulation, privacy policy content was obscure and difficult to understand with unclear frameworks, and 91% of APPs exhibited excessive collection of personal information. Scores for aspects such as personal information retention periods, storage locations, and security emergency response measures ranged only from 1.2 to 1.5 points (out of 3) [5].

As mobile internet increasingly permeates people's study, work, and daily life, mobile health APPs represent specific applications of mobile APPs in the medical and health field. Compared with ordinary mobile applications, mobile health APPs involve not only identity information such as name, date of birth, gender, occupation, phone number, and email address, but also health diagnosis and treatment information obtained during the provision of disease prevention, physical examination, diagnosis, and treatment services [6]. Therefore, privacy concerns are more significant and security requirements are higher. In recent years, research on the practical application and evaluation of privacy protection policies for mobile health APPs has attracted attention from domestic and international researchers. Researchers have investigated and analyzed the privacy policies of mobile health APPs from different perspectives, covering areas such as medical health consultation, chronic disease management, medication management, and home monitoring. Evaluation dimensions include collection, storage, use and access, sharing and transfer, as well as consultation and feedback. Analytical methods primarily consist of content analysis, text analysis, and comparative analysis, as shown in Table 1 .

However, relevant studies at home and abroad indicate that mobile health APP privacy policies suffer from poor readability and generally low overall scores. A. Sunyaev et al. studied 600 mobile health application privacy policies and found that only 30.5% had privacy policies, which required university-level literacy to read, while 66.1% of privacy policies were not specific to the application's own functions [7]. B. C. Zapata et al. analyzed and evaluated 24 mobile health APPs containing patient electronic medical records from six aspects: privacy policy access, change notification, authentication mechanisms, data encryption, security standards and legal norm constraints, and third-party authorization, finding that all 19 privacy policies failed to fully comply with the assessed template characteristics [8]. A. Sunyaev et al. discovered that most fitness and health APPs collect personal information without user informed consent [9]. Additionally, 48.8% of diabetes management mobile APPs share users' personal health information with third parties [8].

Domestic research on mobile health APP privacy policy evaluation primarily appears in comprehensive surveys. In a 2018 survey of privacy policy transparency among 1,000 common APPs, although medical and health APPs had relatively higher transparency, their score was only 42.2 out of 100 [11-12]. Analysis of existing research reveals that foreign studies on mobile health APP privacy policy evaluation are relatively abundant, while domestic research is scarce and mostly included in comprehensive surveys, lacking large-sample privacy policy survey conclusions specific to the mobile health APP domain. Therefore, this study constructs a privacy policy evaluation index system to assess the text quality of privacy policies for mainstream mobile health APPs in Android app stores, providing policy recommendations to further promote the healthy development of mobile health APPs in China, enhance industry self-regulation, and strengthen government supervision effectiveness.

2. Research on the Current Development Status of Mobile Health APP Privacy Policies

2.1 Research Subjects

According to Kantar Worldpanel ComTech's mobile communication consumer index from June 2019, Android accounted for 79.9% of China's smartphone operating system market share, iOS accounted for 19.7%, and others accounted for only 0.4% [21]. Furthermore, comparison revealed that the top 200 mobile medical and health APPs in the iOS store all had Android versions. Therefore, this study selected mobile health APPs from the Android app store as research subjects. Based on differences in service content, this study categorized mobile health APPs into three types: mobile health, mobile medical, and internet hospital mobile terminals. (1) Mobile health APPs primarily include functions such as health management, fitness exercise, and chronic disease management, examples include Keep, Mi Fit, Codoon, and Daily Yoga. (2) Mobile medical APPs primarily include appointment registration and online consultation

functions, with sponsoring entities being third-party platforms such as Ping An Good Doctor, No. 1 Pharmacy, WeDoctor, and Ali Health. (3) Internet hospital mobile terminal APPs are primarily mobile applications of offline physical hospitals, with both users and developers being offline physical hospitals, such as Children's Hospital Registration, China Medical University First Hospital, and Zhejiang Second Hospital Good Doctor.

In January 2019, this study conducted three rounds of screening for mobile health APPs in the Android app store. First, 589 APPs with more than 10,000 downloads as of December 31, 2018, were selected. Next, APPs without independent privacy policies or privacy statements were eliminated, collecting 269 APPs with privacy policy texts. Then, APPs with duplicate privacy policy texts (where multiple APPs under the same company shared one privacy policy) were removed, ultimately obtaining 104 APPs with independent privacy policy texts. Among these, 42 were mobile health APPs, 52 were mobile medical APPs, and 10 were internet hospital APPs, as shown in Table 2 .

2.2 Main Research Content and Conclusions

This study primarily employed content analysis, a research method that provides objective, systematic, and quantitative descriptions of literature content [22]. It quantifies qualitative information by categorizing content into predefined categories. The literature samples for this study were the privacy policy texts of 104 Chinese mobile health APPs obtained through three rounds of screening. Researchers saved the 104 privacy policies as text files while recording the collection location, download volume, and user ratings of the privacy policies.

To ensure consistency and reliability of the analysis, two researchers independently measured the data, achieving over 95% consistency, indicating good reliability of the analysis results.

In terms of specific indicator settings, this study found that relevant research and the "Specification" have extended personal privacy information security protection throughout the entire data lifecycle, including production, collection, storage, processing, sharing, utilization, and feedback. Therefore, this study constructed first-level indicators for the mobile health APP privacy policy evaluation system from the perspective of the data lifecycle, including six dimensions: privacy policy attributes, personal information collection, storage, use, sharing, and feedback. Based on this foundation and 对照《规范》要求, second-level and third-level indicators were generated to examine mobile APP operators' understanding and implementation of the "Specification" at each stage of the data lifecycle, identify the balance of rights and obligations regarding personal privacy information between service providers and users, and analyze how the data lifecycle radiates into personal privacy information protection practice. Investigating mobile health APP privacy policies through a data lifecycle-based index system can provide clearer understanding of the current state of user privacy protection and identify risk areas in mobile health APPs.

2.2.1 Privacy Policy Length, Update Frequency, and Design Principles Visibility and readability are important compliance standards for privacy policies. This study measured visibility by investigating the location of privacy texts and assessed readability by examining privacy policy text length, key point directories, update status, and design principles. If a privacy text is too short, it may affect the completeness of the privacy policy to some extent; if it is too long and the content is obscure and difficult to understand, it may hinder user reading and comprehension. The survey found that the average length of privacy texts from sampled APPs was 4,190 characters, with a median of 2,846 characters. Only 19 APPs provided key point directories for privacy policies to facilitate reading. Regarding the most recent update time, among the 104 sampled mobile health APPs, only 22 (21.15%) marked dynamic update times for their privacy policies, with 17 having update times after 2018.

Once users register and use an APP, the software provider becomes the actual controller of users' personal health information. The "Specification" requires privacy information controllers to follow principles including consistency of rights and responsibilities, clear purpose, selective consent, minimal sufficiency, ensuring security, subject participation, and transparency. The study found that 10 sample APPs mentioned adherence to the user selective consent principle, 11 guaranteed reasonable use of user personal information, and one APP named "Yishitong" mentioned integrating privacy protection into product design as a fundamental information security principle.

2.2.2 Personal Information Collection Stage During the information collection stage, when users download and register for mobile health APPs, platforms may collect personal identity information, communication information, personal health physiological information, personal property and payment information, and location and address information. Mobile health APPs with robust privacy protection policies should inform users about the types and purposes of collected information; otherwise, they risk personal privacy information leakage. Research results show that among the 104 APPs, 61 (58.65%) informed users about the purpose and method of collecting their personal information; 30 (28.85%) did not specify the types of personal information collected; 70 (67.31%) collected personal identity information; and 39 (37.50%) collected personal health physiological information data, as shown in Table 3 .

Cookie technology and other automated tools are small data files used by software developers or operators to track user traces, facilitating the collection of user characteristic information and understanding, analysis, and management of user behavior. Therefore, when mobile health APPs use tools like Cookies, they should provide detailed descriptions of their usage purposes and refusal options. The survey found that 57 APPs (54.81%) explicitly stated they would use Cookies, with 44 informing users of the purpose of using Cookie technology. Regarding user self-control, 40 APPs indicated that users could refuse Cookie technology, and 37 informed users of the consequences of refusal, namely being

unable to use services dependent on Cookies or needing to change user settings.

In addition to the types of information collected, operators must also specify the target groups for information collection. Generally, mobile health APPs primarily serve adults. Without guardian consent, minors should not independently create and use accounts. When involving minor-related information, collection, use, and disclosure should only occur when legally permitted and with explicit guardian consent, while information of minors without guardian consent should be deleted. The survey found that 44 APPs (42.31%) explicitly marked provisions for minor information protection in their privacy policies, clearly stating that when collecting minor information, consent from the minor themselves or their guardian should be obtained. Among these, 9 APPs provided detailed age definitions for minor users based on civil capacity: 7 APPs considered individuals under 14 years old as minors, and 2 considered those under 16 as minors. Additionally, to ensure operability of minor information protection, 5 APPs including "Daoyitong" explicitly stated in their privacy policies that written guardian consent must be provided before minors can register and use the APP.

2.2.3 Personal Information Storage Stage During the user information storage stage, software developers and operators should provide detailed explanations in their privacy policies regarding information storage locations, storage duration, and protection measures. Survey results show that 33 APPs explicitly informed users about storage locations. Since the selected mobile health APPs all target domestic users, they generally promised to store users' personal information on domestic servers and not transfer it globally. Among the 104 APPs, 16 informed users about storage duration, stating they would only store users' personal information for a reasonable period and would delete personal information or conduct anonymization processing after user account cancellation and beyond a regret period. For example, "Dingdang Kuaiyao" explicitly stated it would delete or anonymize personal information one month after user cancellation.

Regarding information storage security measures, 61 APPs (58.65%) included one or more information security storage protection measures in their privacy policies. These measures generally include: (1) preventing improper use or unauthorized access, public disclosure, use, modification, damage, loss, or leakage of personal information; (2) preventing malicious attacks on personal information through encryption technology and anonymization processing; (3) establishing dedicated security departments, security management systems, and data security management processes; (4) striving to avoid collecting irrelevant personal information and retaining personal information only for reasonable periods; (5) actively taking protective measures and cautiously providing personal information to others; (6) irregularly updating and publicly releasing security risk and personal information security impact assessment reports; and (7) developing emergency response plans and immediately activating emergency plans when

user information security incidents occur to prevent and minimize the impact and consequences of such incidents. The number of APPs adopting various security storage protection measures is shown in Table 4 .

For emergency response to personal information security incidents, 24 APPs (23.08%) provided response plans, stating they would promptly inform users of relevant information, including basic information about the infringement incident and potential impacts, measures already taken or to be taken by the platform, suggestions for users to independently prevent and reduce risks, and remedial measures for users. Among these, 20 APPs (19.23%) stated they would also promptly report to national information security departments, and 13 APPs (12.50%) expressed willingness to assume legal responsibility for user privacy information leakage.

2.2.4 Personal Information Use Stage During the information use stage, users may disclose their health privacy information through health and medical consultations between doctors and patients or among patients. On one hand, users may proactively disclose personal health information to doctors to obtain personalized, high-quality medical and health information. On the other hand, users may publish their medical experiences and other personal health information through topics, posts, and articles on social media to gain attention and interact with other users in health communities. Pew Research Center survey results show that in 2012, approximately 26% of American internet users read about others' experiences with health or medical issues, and about 16% searched for people with the same health problems [23].

During the information use stage, users have certain control rights over their information, generally including accessing, deleting, and correcting personal information; independently choosing and controlling personalized recommendation information; changing authorization scope or revoking authorization; and canceling accounts. Survey results show that 44 APPs (42.31%) explicitly stated in their privacy policies that users could query, correct, or delete personal information; 33 APPs (31.73%) informed users of their right to cancel accounts; and 24 APPs (23.08%) indicated that users could change authorization scope or revoke authorization, with 23 informing users of the process or consequences of changing or revoking authorization, as detailed in Table 5 .

The "Specification" stipulates that individuals have the right to refuse and terminate mobile APPs' use of personal information. However, most APPs (71, accounting for 68.27%) did not completely terminate the use of user information according to user wishes but instead continued to use users' personal information after desensitization or de-identification processing.

2.2.5 Personal Information Sharing Stage Some service providers collaborate with third-party pharmaceutical and device websites, health consultation websites, or academic research institutions to develop additional services to increase traffic and user stickiness. These extra services increase the risk of

leakage of users' personal health information. Meanwhile, due to the significant commercial value of personal health information, it may be illegally traded or stolen by third parties outside of doctors, patients, and platforms through gray interest chains in "information secondary trading markets."

The "Specification" stipulates that personal information should not be transferred or shared in principle. When personal information controllers must transfer or share information, they should fully emphasize the risk of information leakage in this process. Survey results shown in Table 6 indicate that among the 104 APPs, 13 had affiliated institutions, and 9 APPs would share users' personal information with their affiliated institutions; 86 APPs (82.69%) would share user data with third parties, primarily in nine situations: user authorization, legal and regulatory requirements, sharing with affiliated companies and partners, academic research, handling disputes or controversies with others, programmatic advertising push, health advice upon user request, and helping log in to third parties. Regarding whether Cookies were shared, 4 APPs explicitly stated they would share Cookies with affiliated institutions or third parties.

Regarding specific circumstances of information disclosure, 39 APPs stated they would publicly disclose personal information with user informed consent; 63 APPs would disclose user information to society when users violate laws and regulations or when required by law; and 17 APPs stated they would publicly disclose user-related information in penalty announcements when users engage in violations and fraudulent behavior. Regarding handling of special circumstances, 75 APPs (72.12%) indicated that users needed to consent to personal information disclosure to obtain certain specific services. 90 APPs (86.54%) stated they would disclose user information when required by law or when protecting public rights and interests. Additionally, when user authorization, legal requirements, compliance with signed agreements, or APP operator business transfer, acquisition, and merger occurred, 42 APPs stated that personal information databases could be transferred to third parties, with 28 APPs stating that the receiving party would also comply with the current privacy policy or formulate stricter policies.

2.2.6 Information Consultation and Feedback When users have questions about privacy policies, they can contact operators through phone numbers, email addresses, or physical addresses provided by the APP. Therefore, privacy policies should explicitly indicate channels and methods for information consultation. Survey results show that 47 APPs (45.2%) stated they could handle questions and complaints and provided contact channels. Three APPs including "Huayitong" also established dedicated departments or personnel for personal information protection. However, regarding promises of complaint response time limits, only 19 APPs provided timeframes, ranging from 5 to 30 working days. Nine APPs including "Jiankangzhilu" indicated in their privacy policies that users could file lawsuits in competent courts when they believed their legitimate rights and interests were infringed. "Qingsongchou" and "Ding-

dang Kuaiyao" also provided other complaint or reporting channels, such as regulatory departments for cyberspace administration, telecommunications, public security, industry and commerce, and civil affairs.

2.2.7 Construction of Evaluation Index System and Evaluation Results To more comprehensively compare the privacy policy quality of the 104 mobile health APPs, this study constructed a comprehensive privacy policy evaluation system from the perspective of the data lifecycle, combining existing research and the "Specification" content. Based on the hierarchical and opposing relationships among various indicator options, scores were assigned to each option, with each third-level indicator given equal weight. When options were "yes" or "no," a value of 1 was assigned for meeting the condition and 0 for not meeting it. When multiple options existed, each option was assigned equal 分值, with corresponding scores given for meeting one option. For example, indicator C11 has three options, meeting one scores 1/3, meeting two scores 2/3, and meeting all three scores 1 point, as shown in Table 7 . The comprehensive count of third-level indicators met by each APP represents each APP's measurement result, which was converted to a percentage scale to obtain each APP's final score.

Comprehensive evaluation of the privacy policies of 104 mobile health APPs revealed that overall performance in user privacy protection policies was suboptimal. As shown in Figure 1 [Figure 1: see original paper], scores exhibited a non-normal distribution. With 100 as the full score, the average score was 44.58, indicating that current privacy policy protection effectiveness has not reached a satisfactory state (see Table 8 for details). Seventy-seven mobile health APPs scored between 0-60 points, accounting for 74.04% of the total; 14 scored between 61-80 points, accounting for 13.46%; and 13 scored above 80 points, accounting for 12.50%.

Regarding the evaluation scores of the index system, third-level indicators with lower scores included the "update time" indicator in the privacy policy dimension (21 points); the "types of information security incident response measures" indicator in the data storage dimension (15 points); the "consequences of users exercising choice rights" indicator in the data use dimension (22 points); and "whether sharing data with affiliated institutions is explained" and "whether third-party Cookie usage is explained" in the data sharing dimension, scoring 13 points and 7 points respectively.

3. Recommendations for Improving Mobile Health APP Privacy Policies

With the implementation of the national standard "Personal Information Security Specification" (GB/T 35273-2017), standardization and supervision of privacy policies for mobile health APPs have become stricter. Therefore, it is necessary to optimize APP privacy policy design, promote standardized formu-

lation of mobile health APP privacy policies, establish evaluation standards and regulatory mechanisms for privacy policy quality, and improve laws and regulations for protecting personal health privacy information to ensure user safety and effectiveness.

3.1 Enhancing the Visibility and Readability of Privacy Policy Texts

With the development of "Internet + Healthcare," users increasingly utilize mobile health APPs. However, survey research reveals that current privacy protection effectiveness of mobile health APPs is unsatisfactory, with phenomena of excessive collection and misuse of personal health privacy information. Therefore, strengthening the design and usage norms of mobile health APP privacy policies is needed to enhance user privacy protection levels. Visibility and readability are important compliance standards for privacy policies and constitute crucial content for evaluating privacy policy completeness [5]. Regarding visibility, operators need to mark privacy policy entries in prominent locations with effective links to privacy policy texts. Titles should include the word "privacy," such as "Privacy Policy," "Privacy Statement," "Privacy Protection," "Privacy Rights Guidance," or "Personal Privacy Information Protection." Regarding readability, privacy policies should be designed according to the framework in the "Specification"; they should be as standardized and clear as possible to facilitate reading, with directory indexes provided to prompt content and timely updates.

3.2 Further Optimizing Privacy Protection Policies for Mobile Health APPs

First, privacy policies must clearly define the types and purposes of personal health information collected according to service content. Survey results show that most mobile health APP privacy policies define personal health information (including identity information and health diagnosis and treatment information). However, as mobile health APP service models and content gradually innovate, new service content involving personal health information should be expanded and updated according to the personalized services provided. For example, some foreign doctor-patient social APPs have expanded protected personal health information to include consultation and interaction information between patients and doctors or health service providers. Additionally, some European and American countries have also included identifiable deceased persons' information within the scope of personal health information protection [24].

Second, personal health information should be incorporated into full lifecycle security protection and clarified through privacy policies: (1) In the information generation stage, privacy policies need to specify applicable laws and regulations. For example, European and American mobile health APPs indicate they operate under HIPAA or GDPR frameworks [25], while Chinese mobile health APPs lack clear markings. (2) In the information collection stage, principles of clear

purpose, selective consent, and minimal sufficiency should be followed to avoid excessive collection of personal information; the types, purposes, and methods of information collection should be detailed, and security risk assessments should be conducted. (3) In the information storage stage, to ensure secure storage of personal information, retention periods for personal health information should be improved. For example, the mobile application of UK-based Babylon Health company stipulates that general practitioner records are retained for 10 years after patient death or permanent departure from the country, and obstetric records are preserved for 25 years after the birth of the last child [26]. (4) In the information use stage, operators must inform users in advance before using their information to avoid excessive authorization; age limitations should be implemented when collecting information from elderly and minors, with targeted safety knowledge popularization. The U.S. Food and Drug Administration (FDA) requires some mobile health APPs to provide users with an annual report detailing the types of information collected and used, and if information is shared with third parties, the names of third-party institutions and types of shared information must also be provided [27]. (5) In the information sharing and feedback stage, users have the rights to access, correct, delete, and cancel personal accounts. When operators need to share or transfer user personal information, de-identification or anonymization processing should be adopted and explained in the privacy policy. For APPs involving cross-border business, applicable international privacy policy frameworks should also be published to ensure information security when transferring data between different countries. (6) In the information feedback stage, privacy policies must specify specific operational processes and provide communication channels for consultation and feedback.

3.3 Standardizing Evaluation and Supervision Mechanisms for Mobile Health APP Privacy Protection

Protecting user privacy information involves not only formulating privacy terms but also implementing the specific content promised in those terms. However, unified evaluation standards and regulatory mechanisms for mobile health APPs are currently lacking. Compared with other industry applications, mobile health APPs face relatively higher information security risks. Information asymmetry exists in medical services, and medical service providers and operators may collect excessive privacy information from patients during diagnosis and treatment processes that is not easily detected. Therefore, the principles of "inclusive prudence, safety and order" must be followed to strengthen quality and data security supervision of mobile health APPs, effectively prevent risks, ensure safety during development, and maintain bottom lines. Given the particularity of health privacy information, relevant departments should construct evaluation systems and regulatory mechanisms for internet medical health and mobile APP privacy protection policies: regularly evaluate the standardization and operability of privacy policies, use technical standards to detect the security and stability of mobile health APPs, and remove non-compliant APPs; supervise and urge

operators to implement corporate 主体责任, establish dedicated personal information security departments and personnel to respond to information security incidents; strengthen internal management, regularly review operational permissions of internal staff, emphasize signing of confidentiality agreements upon resignation, and conduct information security training and assessments to prevent staff from leaking user medical health data due to economic incentives or curiosity.

3.4 Improving the Legal Environment for Protecting User Health Privacy Information

Protecting the privacy and security of personal health information depends not only on the formulation and implementation of privacy policies but also requires regulating the use of user health information from a legal perspective, thereby ensuring both protection of users' legitimate rights and better promotion of "Internet + Healthcare" development. However, compared with the U.S. "Consumer Privacy Protection Act" and the EU's "General Data Protection Regulation," China's "Specification" lacks mandatory force and professional specificity, providing insufficient guidance for protecting personal health privacy information [6]. Therefore, first, the content of personal health information must be clearly defined at the legal level, clearly delineating the scope of protection during collection, use, sharing, management, transfer, and disclosure of health information on the internet and mobile APPs. Second, ownership of personal health information must be clarified. Users share personal health information on mobile health APPs but rarely actively manage their own information. The permissions of medical institutions and operators to use and dispose of user privacy information require clear definition. Finally, due to information asymmetry between users and operators, users cannot timely learn whether their information has been leaked and the severity of leaks when information security incidents occur. Therefore, laws should clearly define operators' evidence collection obligations and establish clear rights relief mechanisms to ensure that information subjects can obtain certain compensation when experiencing information leakage and resulting harm, protecting users' legitimate rights and interests after security incidents.

References

[1] Ma Xiaowei. Accelerating the innovative integration development of internet healthcare to help Healthy China construction reach a new level[J]. Current Affairs Report (Party Committee Center Group Study), 2018(5): 43-55.

[2] Zhang Xiulan. Research on Network Privacy Protection[M]. Beijing: Beijing Library Press, 2006: 113-128.

[3] Wang Xiwei, Xiang Mengmeng, Zhang Changliang, et al. Domestic and international research trends and development trends of information privacy in the new media environment[J]. Library and Information Service, 2017, 61(15):

6-14.

[4] He Peiyu, Ma Yaxin, Tu Meng. Research on Web browser user privacy security policy issues and countermeasures[J]. Library, 2019(2): 19-26.

[5] China Consumers Association. Evaluation report on personal information collection and privacy policies of 100 APPs[EB/OL]. [2019-06-28]. http://www.cca.org.cn/jmxf/detail/28310.html.

[6] He Lan. Value conflicts and governance in the development and protection of personal health information[J]. E-Government, 2018(1): 92-99.

[7] Sunyaev A, Dehling T, Taylor PL, et al. Availability and quality of mobile health app privacy policies[J]. Journal of the American Medical Informatics Association, 2014, 22(1): e28-33.

[8] Zapata BC, Ninirola AH, Fernandez-Aleman JL, et al. Assessing the privacy policies in mobile personal health records[C]//IEEE. 2014 36th annual international conference of the IEEE engineering in medicine and biology society. Chicago: IL, 2014: 4956-4959.

[9] Mariam B, Ali I, Fernandez-Aleman JL, et al. Evaluating the privacy policies of mobile personal health records for pregnancy monitoring[J]. Journal of medical systems, 2018, 42(8): 1.

[10] Sunyaev A, Dehling T, Taylor PL, et al. Availability and quality of mobile health app privacy policies[J]. Journal of the American Medical Informatics Association, 2015, 22(4): 28-33.

[11] Feng Jiacheng, Gao Duxiu, Chen Hongmiao. Research on development countermeasures for sports health APPs based on prevention of user privacy leakage[J]. Journal of Jilin Sport University, 2016, 32(6): 63-68.

[12] Luo Weina, Li Shu, Wang Chenxi, et al. Research on mobile medical network security supervision strategies[J]. China Medical Devices, 2017, 32(6): 20-22, 31.

[13] Croll PR. Determining the privacy policy deficiencies of health ICT applications through semi-formal modelling[J]. International journal of medical informatics, 2011, 80(2): e32-38.

[14] Rowan M, Dehlinger J. A Privacy policy comparison of health and fitness related mobile applications[J]. Procedia computer science, 2014, 37(9): 348-355.

[15] Zhu Ying. Research on mobile APP privacy protection policies in China—Based on analysis of 96 mobile APPs[J]. Jinan Journal (Philosophy and Social Sciences), 2017, 39(12): 107-114.

[16] Liu Jiao, Bai Jing. Comparative study of Chinese and foreign mobile APP user privacy protection texts[J]. Journal of Shantou University (Humanities and Social Sciences Edition), 2017, 33(3): 82-87.

[17] Powell AC, Singh P, Torous J. The complexity of mental health app privacy policies: a potential barrier to privacy[J]. JMIR mHealth and uHealth. 2018,

6(7): e158.

[18] Parker L, Halter V, Karliychuk T, et al. How private is your mental health app data? an empirical study of mental health app privacy policies and practices[J]. International journal of law and psychiatry, 2019, 64(3): 198-204.

[19] Rosenfeld L, Torous J, Vahia IV. Data security and privacy in apps for dementia: analysis of existing privacy policies[J]. The American journal of geriatric psychiatry, 2017, 25(8): 873-877.

[20] Robillard JM, Feng TL, Sporna B, et al. Availability, readability, and content of privacy policies and terms of agreements of mental health apps[J]. Internet interventions, 2019, 17(9): 1.

[21] Kantar: Smartphone operating system market share[EB/OL]. [2019-10-07]. https://www.kantarworldpanel.com/cn/smartphone-os-market-share/.

[22] Ma Wenfeng. Analysis of the application of content analysis in social science informatics[J]. Information Science, 2000(4): 346-349.

[23] Susannah F. The social life of health information[EB/OL]. [2019-07-15]. http://www.pewresearch.org/fact-tank/2014/01/15/the-social-life-of-health-information/.

[24] Jiang Wen. Review and enlightenment of basic elements of foreign personal health information[J]. Chinese General Practice, 2016, 19(30): 3652-3656.

[25] Li Zhuozhuo, Ma Yue, Li Mingzhen. Personal privacy information protection from the perspective of data lifecycle—Content analysis of mobile APP service agreements[J]. Information Theory and Practice, 2016, 39(12): 63-68.

[26] Babylon health privacy policy[EB/OL]. [2019-10-07]. https://www.babylonhealth.com/terms/privacy.

[27] Carbon health privacy policy[EB/OL]. [2019-10-07]. https://carbonhealth.com/privacy-policy.

Author Contribution Statement:

Ma Chengyu: Topic selection and formulation, research framework construction, paper writing;
Liu Qiankun: Literature review and data collection, paper revision.

Research on the Privacy Policy's Evaluation and Empirical Study of Mobile Health Applications

Ma Chengyu, Liu Qiankun
Department of Health Management and Policy, School of Public Health, Capital Medical University, Beijing 100069

Abstract:
[Purpose/Significance] To analyze the safety situation of privacy policy based on popular mobile health applications and propose to improve the privacy

protection mechanism. [**Method/Process**] 104 privacy policy texts of mobile health applications were selected as research objects through three rounds of screening. The content of the text was analyzed based on the content analysis method, and evaluated by a comprehensive evaluation system. [**Result/Conclusion**] The overall evaluation score of mobile health apps' privacy policy is relatively low, with the average score of 44.58 (100 full marks). Privacy policy needs to be improved in terms of content normatively and completeness. Some apps have the situation of excessive information collection and personal health privacy data abuse. The suggestions are proposed from 3 aspects, including optimizing the privacy policy design of apps, standardizing the privacy policy evaluation and supervision mechanism, and improving the legal environment for protecting users' health privacy information.

Keywords: privacy policy; mobile health; privacy protect; assurance mechanism

---

Next Issue's Table of Contents

Note: Figure translations are in progress. See original paper for figures.