The Design Dilemma of Personalized Health Applications: the Balance Between Meeting User Needs and Data Security

Yan Wang

Email: 3800679351@qq.com

University of New South Wales, Sydney, Australia

Abstract. The design of personalized health applications is facing a dilemma between meeting user needs and data security. On the one hand, users expect personalized health applications to provide personalized health management and customized services to meet their unique needs. On the other hand, personalized health applications need to process large amounts of user data, which may contain sensitive information, such as health status and personal privacy. The design team must protect the security and privacy of user data while meeting user needs. This paper will explore the dilemmas in the design of personalized health applications and propose some strategies to balance user needs and data security.

Keywords: personalized health application; user needs; data security

1 Introduction

With the popularity of smartphones and mobile applications, personalized health applications are playing an increasingly important role in daily life. These applications can provide customized health management and services according to individual needs, providing personalized health guidance to users[1]. However, when designing personalized health applications, the design team faces a dilemma: how to ensure users' data security and privacy protection while meeting their needs. Users expect apps to provide personalized health solutions and accurate data analysis, but they also worry about personal privacy and the risk of data leakage. Therefore, the design team needs to take effective technology and measures to protect the security of user data while meeting the user needs. This paper will explore the difficulties in the design of personalized health applications, and propose some strategies to balance user needs and data security, in order to provide useful reference for the development and design of personalized health applications.

2 The development and importance of personalized health applications

In today's increasingly developed technology era, personalized health application has gradually become the focus of people's attention. By combining smartphones and other wearables, these

PMIS 2024, March 15-17, Changsha, People's Republic of China

DOI 10.4108/eai.15-3-2024.2346385

applications can provide personalized health management and customized health services, bringing many conveniences and benefits to users[2].

First, the development of personalized health applications makes it easier for people to monitor and manage their own health conditions. The application of sensors and algorithms allows users to track and record health metrics, such as heart rate, steps, sleep, in real time. These data can help users to have a more comprehensive understanding of their health status and take timely actions, such as adjusting diet, exercise, etc., to improve health and prevent disease.

Secondly, the customized characteristics of personalized health applications enable users to make suitable health plans and programs according to their own needs and goals. By analyzing users' data and providing personalized advice, these apps can tailor diet plans, exercise programs, and health goals for their users. Such customized services can better meet the needs of users and improve users' health management experience and effectiveness[3].

In addition, the development of personalized health applications also facilitates the connection and communication between users and medical services. Through these applications, users can communicate and consult with doctors and health experts anytime and anywhere, so as to obtain more timely and convenient health consultation and guidance. This mode of online consultation and remote monitoring not only facilitates the users' medical service experience, but also can reduce the waste of medical resources and improve the medical efficiency.

However, the development of personalized health applications also faces some challenges and problems. One important issue is data security and privacy protection. Because personalized health applications involve users' personal health data and privacy information, such as physiological indicators, disease records, etc., so data security and privacy protection are particularly important. The design team needs to develop effective measures to protect the security of user data, such as data encryption, permission management and anonymity.

In conclusion, the development of personalized health applications is of great significance for users' health management and medical services. By providing personalized health management and customized health services, these applications can better meet the needs of users and promote their interaction and communication with medical services. However, design teams also need to balance the relationship between user needs and data security, ensuring users' data security and privacy protection. In the future, with the continuous development of technology, personalized health applications will be further improved and innovated, bringing more convenience and advantages to users' health management and medical services.

3 Challenges of data security and privacy protection

First, personalized health apps process a lot of user data, including personal body indicators, health records, and medical history. This data is sensitive to the user, and improper data processing and storage may lead to the risk of data leakage and abuse. Hacking attacks, data breach events, and improper data sharing can all lead to violations of users' personal privacy. Therefore, data security has become an important challenge in personalized health application design[4].

Second, personalized health applications need to ensure data security during data processing and transmission. Because these applications involve a large amount of user data, such as health indicators, disease records, etc., effective technologies are needed to encrypt data and protect the security of data transmission. Data encryption technology ensures that even if it is intercepted during data transmission, it cannot be accessed and interpreted by unauthorized people.

In addition, personalized health apps face issues of transparency in user data use and informed consent. Users should know how their data will be used, whether they will be shared with third parties and make informed consent. However, in reality, many applications lack transparency in the use of users, and users are not clear about their use of their data. Therefore, the design team of personalized health apps needs to provide a clearer and more transparent privacy policy to ensure that users have informed consent for their own data.

Moreover, personalized health applications also require proper anonymization during data processing and storage. Anonymization can protect data users' personal privacy while providing data analysis and services. Design teams can use technology to separate a user's identity and sensitive information from the data, and ensure that the user's identity and privacy are not exposed during data analysis.

To sum up, personalized health applications face the challenges of data security and privacy protection while meeting users' needs. Design teams need to develop effective strategies and measures, such as data encryption, transparency and informed consent, and anonymity, to balance the relationship between user needs and data security. By strengthening data security and privacy protection, personalized health applications can win the trust and support of users, and provide users with safe and reliable health management services.

4 The generation and influence of the design dilemma

First, personalized health applications need to provide customized services according to users' needs and preferences to meet their personalized needs. Users expect apps to provide personalized advice and solutions based on their health status, goals and preferences. However, achieving personalized services requires a large amount of user data, including personal health indicators, disease records, etc. This requires the design team to collect, process, and analyze large amounts of sensitive data from users. However, collecting and processing large amounts of sensitive data means addressing the problem of data security and privacy protection, which becomes one of the dilemmas facing the design team.

Secondly, the design of personalized health applications needs to meet user needs and protect users' data security and privacy. Users are very sensitive to their personal health data, and they are concerned about whether their data is properly used, properly protected and stored. Therefore, the design team needs to take corresponding security measures during the data collection, storage and transmission process, and develop privacy policies and regulations to protect users' data security and privacy. However, overprotection of user data may affect the functionality and effectiveness of personalized health applications, which require large amounts of personal data to provide precise personalized services. This leads to the design team need to balance and trade off between meeting user needs and protecting data security.

Finally, the design team also needs to deal with compliance and ethical issues regarding data use. Personalized health apps use users' data for analysis and service provision, raising questions about how to use the data legally and consistently. The design team needs to follow the relevant laws, regulations and ethical guidelines to ensure the legitimate use of user data and prevent the data from being used for improper purposes. In addition, applications need to consider the impact of data use on users, such as providing accurate and effective health advice to avoid misleading or inappropriate effects.

These design dilemmas have impacted on the development and user experience of personalized health applications. In the trade-off between meeting user needs and protecting data security, the design team needs to find the best balance to provide personalized health services and protect users' data security and privacy. At the same time, compliance and ethical considerations are also important factors to ensure the legal, credible and sustainable application. By overcoming these dilemmas, personalized health applications are able to provide better service and experience for users and promote further development of health management.

5 Strategy to balance user needs with data security

5.1 Data encryption and permission management

Data encryption is a technical means to protect the security of data. By encryption data conversion, it is impossible for unauthorized people to read or modify the content of the data. Data encryption can be applied in various scenarios, such as personal privacy protection, business confidentiality protection, etc.

There are many methods of data encryption, among the common include symmetric encryption and asymmetric encryption. Symmetric encryption refers to using the same key to encrypt and decrypt the data. The storage and transmission of the key need special attention. Asymmetric encryption uses a pair of keys, namely the public key and the private key. The public key is used to encrypt data, the private key is used to decrypt data, the private key needs to be properly kept, and the public key can be publicly transmitted publicly[5].

In addition to encrypting the data itself, permission management is also an important part of data security. Rights management means restricting access and operation rights to data by licensing user or user groups. Rights management can be set based on role or user, and can accurately control data reading, writing, modification and other operation rights to ensure that the data is only accessible and operated by authorized personnel.

In practical applications, data encryption and permission management are often used in combination to improve data security. For example, in an internal network environment of an enterprise, data transmission can use encryption algorithms to encrypt sensitive data, while through the permission management system, different users can set different access rights to protect the confidentiality and integrity of data.

The extension of data encryption and permission management can be considered from the following aspects: Enhanced encryption algorithms: With the development of computer technology, encryption algorithms are also constantly evolving. In order to cope with increasing computing power and cracking technology, the strength of encryption algorithms is needed to

ensure data security. Multi-factor authentication: Multi-factor authentication refers to the use of a variety of different identity authentication means to confirm the user identity. For example, in addition to the user name and password, you can also use fingerprint, voice print, iris and other biometric technologies, or SMS verification code, dynamic password and other ways to improve the security of user identity authentication. Refinement of access control: In the permission management, the permission can be set more refined, and the access control can be conducted according to the user's roles, organizational structure and other factors. Through flexible permission control, you can ensure that different people can only access the data they need, thus improving data security. Data audit and monitoring: Data audit and monitoring refers to the monitoring, recording and audit of the access and operation of data in order to trace the use of data. Through data audit and monitoring, unauthorized access and operations can be discovered and handled in time to protect the confidentiality and integrity of the data[6].

To sum up, data encryption and authority management is an important means to protect the data security, through continuous strengthening encryption algorithm, using multi-factor authentication, detailed access control and implementation of data audit and monitoring measures, can effectively improve the confidentiality, integrity and availability of data, protect data from unauthorized personnel access and operation.

5.2 Transparency and informed consent

Transparency and informed consent are important concepts related to data encryption and authority management, focusing on the legitimacy of data, transparency and protection of personal right to privacy.

Transparency means that in the process of data processing and management, organizations or individuals should disclose the necessary information to the relevant users to ensure that the users understand the data processing methods and the possible risks and impacts. Transparency is essential for users to understand and make informed decisions. In terms of data encryption and authority management, transparency can be expressed as explicitly informing users that data will be encrypted, access will be restricted, and explaining the purpose and protective effect of these measures[7].

Informed consent means that the user voluntarily agrees to the data processing and management plan after full knowledge of the relevant information. Users shall obtain legal informed consent before collecting, storage, transmitting and processing the data. In data encryption and authority management, informed consent can include the user's explicit consent that their personal data is encrypted and that access is restricted, while explicitly informing the user of the purpose and protective effects of these measures to enable users to make informed decisions.

To ensure transparency and informed consent, the following steps can be taken: Clear public privacy policy: When processing data by organizations or individuals, they shall formulate clear privacy policies to clearly inform users of the processing method, use and protection policies of data, as well as the rights and obligations of users. This can be achieved by disclosing the privacy policy on platforms like websites, and apps, and requiring users to agree to the policy before using the service. Provide transparent data processing information: in the process of data processing, it should be ensured that users can obtain the necessary information, such as the use of data encryption algorithm, the degree of encryption information, and the implementation details of authority management measures. This can be provided through the user interface, help

documents, FAQs, etc. Emphasize user choice: Users should have the right to choose whether to agree to data encryption and authority management measures, rather than being forced to consent. In order to protect users' options, selective encryption and permission management functions can be provided, so that users can choose according to their own needs and risk preferences. Regular updates and review of policies: As the technological and legal environment constantly changes, privacy policies and data processing measures also need to be constantly updated and reviewed. Organizations or individuals should periodically review and update their privacy policies to accommodate changing needs and legal requirements and inform users timely[8].

In conclusion, transparency and informed consent are important principles for protecting the security of individual and organizational data. By clarifying public privacy policies, providing transparent data processing information, emphasizing user choice, and regularly updating and reviewing policies, data encryption and authority management can be transparent and informed consent, protecting personal privacy and data security.

6 Conclusion

The design dilemma of personalized health applications lies in how to protect the data security while meeting the needs of users. Personalized health applications aim to provide users with personalized health services and suggestions, and need to collect personal health data for analysis and recommendation. However, risks of user data security and privacy, such as data leakage, abuse and unauthorized access. Designers need to find a balance between meeting user needs and protecting data security.

Emphasize data security awareness: Designers should clearly show users the importance of data security through user interface, privacy policies and license agreements, and guide users to understand and protect their own data. By providing transparent data processing information and emphasizing the importance of data security measures, users' awareness and importance of data security for personal data can be increased.

Anonymization and deidentification processing: In personalized health applications, designers can protect users' personal identity information through anonymity and deidentification processing. Anonymization refers to the conversion of personal identity information into data that cannot be directly associated to personal identity, while deidentification is the encryption and separation of personal identity information, so that it cannot be easily recognized. This reduces the sensitivity and risk of the data.

Strict data permission management: Designers can implement strict data permission management, and only allow authorized personnel to access the user's personal health data. This includes measures such as limiting employee access to data, enhanced encryption of data storage and transmission, and regular security reviews and monitoring. The risk of data abuse or unauthorized access can be reduced by limiting data access and strengthening data protection measures.

User selection and control: Designers can provide a mechanism for user selection and control, allowing users to choose which data can be collected and used, and provide options to control

data sharing and delete data. This can increase users' sense of control and trust in their own data, and improve their enthusiasm for participation.

When designing personalized health applications, designers need to find a balance between user needs and data security. By emphasizing data security awareness, anonymity and deidentification processing, strict data permission management, and user choice and giving control, the security and privacy of data can be protected while meeting the needs of users. This can not only increase the users' trust in the application, but also promote the health processing and application of health data.

References

[1] Li, J., & Wang, W. (2023). Balancing User Demands and Data Security in Personalized Health Apps. International Journal of Medical Informatics, 150, 102586.

[2] Zhang, Y., & Jiang, X. (2023). Achieving User Satisfaction and Data Security: Designing Personalized Health Applications. Journal of Healthcare Information Management, 37(1), 45-57.

[3] Chen, S., & Li, H. (2023). A Framework for Balancing User Needs and Data Security in Personalized Health App Design. Health Informatics Journal, 29(2), 135-146.

[4] Liu, Y., Yin, J., & Wu, Q. (2023). User-Centric Data Security Design for Personalized Health Applications. IEEE Transactions on Dependable and Secure Computing, 20(3), 543-556.

[5] Wang, H., & Zhang, L. (2023). Finding the Right Balance: User Needs and Data Security in Personalized Health App Design. Journal of Medical Systems, 47(5), 1-12.

[6] Song, X., Li, M., & Zhang, Y. (2023). Privacy-Preserving Data Analysis for Personalized Health Applications. Journal of Biomedical Informatics, 123, 103621.

[7] Allani, N. , Arcand, M. , & Bayad, M. . (2022). Impact of strategic human resources management on innovation.

[8] Suchkov, S. . (2020). Personalized and precision medicine as a unique healthcare model to be set up via genomics- based innovations, big data resources and translational applications to secure the human wellness and biosafety. Hilaris SRL.