User Privacy in Mobile Health Applications

Analysis of e-Pulse application

Tolga Çakmak
Department of Information Management
Hacettepe University
Ankara, Turkey
e-mail: tcakmak@hacettepe.edu.tr

Şahika Eroğlu
Department of Information Management
Hacettepe University
Ankara, Turkey
e-mail: sahikaeroglu@hacettepe.edu.tr

***Abstract*— Mobile health (mhealth) applications that are widely used for many different purposes such as tracking chronical diseases and lifestyle management have many advantages as well as potential limitations and privacy concerns. In this regard, it is seen that the studies with different points of view on the personal data, data protection, and privacy and security features and architectures of these apps are increasing in the literature. This study aims to evaluate the privacy and data protection conditions of the e-Pulse app that is developed by the Ministry of Health in Turkey. In line with this aim, personal data security and privacy conditions of the e-pulse app that is the official mobile health app of Turkey are described with a checklist developed according to the literature review. Privacy and personal data protection issues of the app are highlighted and potential recommendations are discussed in the results of the study.**

Keywords-mobile applications; privacy policies; mobile health applications; data protection; data privacy.

I. INTRODUCTION

Users can do many things that are necessary for the routine life processes with mobile devices and mobile apps, which are being an integral part of daily life. Applications installed on smartphones enable users to benefit from a variety of mobile internet services including personalized services. In recent years, it is seen that mobile apps affect businesses, social life, and lifestyle. The rapidly increasing use of mhealth apps also helps not only to improve the quality of life of the citizens but also to improve health services. mHealth apps that are used by physicians and patients to manage and observe health information, with their features, such as getting blood test results, glucose reading and displaying medical images and medical information convert mobile devices (tablets, smartphones, etc.) into medical devices [1]. In this regard, potential advantages of mhealth apps are stated as offering a fast diagnosis, providing feedback for monitoring health status, promotion of healthy behavior, providing easy access to treatment and rehabilitation, receiving electronic prescriptions, faster access to consent and reducing waiting times [2]. In light of this information, it is possible to describe many mhealth apps as the information or data providers increasing awareness and literacy level about health.

mHealth apps those usage increased especially with wearable medical devices provide many advantages for medical tracking and consent. However, these apps potentially have some limitations and privacy concerns. In this regard, it is seen that many healthcare app providers are not certified by any authority institutions and they do not have training about health information privacy and confidentiality. This is stated as one of the reasons for the concerns [1]. For instance, app providers can request to access users' contacts stored in mobile devices without any permission. When the user allows the app to see or use the GPS data, apps often disclose that this information will be sent to advertising companies. Moreover, it appears that many app users do not know where the information goes or how the developer plans to use it [3]. mHealth apps require many personal data to provide their services. This situation brings the user's privacy and security concerns. These concerns can be listed as monitoring by the unauthorized agents and sharing location or health data to third parties. As a matter of fact, given the distributed and wireless nature of sensor networks, the difficulty of ensuring data security in mobile apps is mentioned in the studies [4]. Privacy violations that may occur in the use of mhealth apps may harm users. Users who are subject to loss of personal data can lose their reputation and social insurance or they can face with employment discrimination [5][6]. At this point, it is very important for the app providers to make efforts to produce beneficial apps and to take precautions for user privacy and confidentiality in the apps considering the potential threats. In addition, it is seen that privacy policies are insufficient level in terms of clarity of data collection, storage, and transmission processes. It would not be wrong to say that the difficulty of the readability and understandability of these policies is another factor for this insufficiency. It is expressed that the main reason for this situation is lack of a standardized format and terminology [1][7][8].

mHealth apps with their potentials have been the subject of many scientific studies in recent years. In this context, it is seen that different models are developed on the reduction of privacy concerns and the improvement of systems in mobile apps. In general, it is seen that different models are suggested in the studies, which emphasize the importance of the reliability of mhealth apps [9]-[11]. There may be privacy issues in the architecture of mhealth apps, which benefit

 ISBN: 978-1-61208-759-7

from significant information communication infrastructures. In this context, one of the most important areas for mhealth apps to reach wider use areas and to utilize their potential benefits more effectively is the security and privacy opportunities offered by these apps for personal data. The privacy and security of mhealth apps can be examined within the framework of three components (such as law, culture/custom, and technology). In addition to the technological safety and user analysis of apps, it is seen that governments and app producers are working on the resources that include guidelines and recommendations for the implementation of privacy and security in apps [12]-[15]. On the other hand, in spite of this guidance published in different sectors, the lack of formal and one-stop standards and guidelines for implementation is stated in the studies [5]. mHealth apps have access to user-identifiable information and personal health information, including diagnosis, symptoms, and use of therapeutic services. Legislation on privacy seeks to protect individuals by requesting consent for the collection, use, disclosure or storage of personal data, including sensitive health information. However, many mobile apps are known to access private data without users' permission.

The usability and effectiveness of mhealth apps are mostly based on user data. These apps can directly request data from users. Furthermore, they can gather user data through a social network connection or location data. It is possible to state that these apps can collect a wider range of data that the user may not be aware of, such as the user's lifestyle, location tracking, social network connections. This situation increases the exposure of users to privacy attacks. In this context, users need to be aware of the increasing privacy risks with ever-changing mobile technology. In mhealth applications, it is seen that there is no comprehensive protection policy for the privacy of personal data. Privacy protections are mostly limited to the protection required by the developer's privacy policy. In this regard, the study shows that only 30% of the most commonly used 600 mhealth apps have a privacy policy [16]. On the other hand, since there is no standard privacy policy content, different applications have different content policies and lack of users' awareness about the issue is an important factor.

In mobile apps, the protection of patient privacy can prevent individuals from particular activities and lead them to remain passive. This may result in the loss of the right of the person to develop his / her material and spiritual existence. Respect for the private lives of persons benefiting from health services is important for the protection of their personal rights, dignity, and personalities. The protection of the patient's information is primarily the responsibility of healthcare providers. Although this responsibility of healthcare providers, users are required to improve their self-efficiency and awareness about privacy issues. Additionally, the state and authority institutions have also vital responsibilities regarding the privacy of the patients, and the implementation of related policies efficiently.

In this study, the privacy policies of the e-pulse application, which was developed by the Ministry of Health in Turkey are analyzed. Accordingly, the methodology of the research is discussed in the second part. The third section presents the findings. In the fourth and final section of the study, conclusion, and recommendations are given.

II. METHODOLOGY

This study aims to analyze privacy policies, data sharing and transmission processes, and privacy settings of the e-pulse mobile app, which is a mobile health application developed by the Republic of Turkey Ministry of Health within the scope of e-government approaches. The main feature of this app is to help citizens for tracking their daily activities such as steps and heart rates and their health records created as a result of the interactions with hospitals. In line with this information, the research questions of the study are as follows:

- What features does the e-pulse application have in relation to the protection of personal data?
- What kind of improvements does e-pulse need in terms of security of personal data and user privacy?

The qualitative research processes were followed in this study. In light of research questions, a checklist is developed according to the literature review. The checklist, which is used to analyze the e-pulse app consists of three sections titled privacy policy document, data sharing and handling, and privacy settings and security. Questions in each section have three answers (such as yes, no, partially) and a textbox for a description of current status. In addition, the checklist and the questions were reviewed through interviews with experts on personal data security. The data were gathered according to two techniques within the scope of content analysis. Firstly, the app was observed and its features used according to questions in the checklist. Secondly, the policy and help documents were analyzed to get deeper answers. Additionally, the gathered data were reported by the titles given in the checklist. Percentage values presented in each section were calculated by dividing the number of completed questions to the number of questions in the section.

III. FINDINGS

In this part of the study, the e-pulse platform, which is a personal health application developed within the scope of e-government applications in Turkey is evaluated in terms of the privacy policy document, data sharing and handling, and personal account information. The findings obtained from the evaluations are presented in this section.

A. Test-bed: e-Pulse App

mHealth apps, which are increasing in number and are widely used by individuals, are developed by governments as well as private developers. They are presented to citizens within the framework of health information systems and e-government applications. According to benefiting from management information systems in healthcare, the electronic pulse (e-pulse) app is developed as a mhealth app by the Ministry of Health in Turkey. The e-pulse app is a mobile and web-based information sharing and retrieval platform that enables citizens to reach all examination information, appointment, diagnosis, treatment, prescription, and medication details, allergy information, laboratory test

 ISBN: 978-1-61208-759-7

results and radiological images with their reports in all health facilities in Turkey. Containing many goals, the app aims to prevent patients from recurrent examinations, to allow both users and physicians to access recent and previous health data, and to make a contribution to the efficiency and effectiveness of health services.

The patients can evaluate the quality of health services they received and express their opinions and complaints by using the app. Patients also can record their data (such as blood pressure, sugar, and pulse data, steps) to their profiles and display this information comparatively. Patients who can access their health data from anywhere with the E-Pulse app will be able to use this data without having to contact the hospitals. The E-Pulse app can be used from a personal computer with its web-based structure. It is also accessible from any smart device with any of the operating systems (Windows Phone, IOS or Android).

B. Privacy Policy Document

At the beginning of the assessment, the privacy document is evaluated in terms of its structure and clarity. It is seen that the application has a privacy document, but this document also includes usage and copyright explanations of the app. Although the scope of the document is not limited to the privacy policy, the document is named as “privacy - data protection statement”. Additionally, this document does not contain a summary and a section of links that help readers to navigate through the document. Moreover, the document does not have the definitions of privacy terms and dates reflecting the latest revisions and updates. Plus, it is seen that the application has a feature to notify users about any updates in privacy conditions.

Secondly, the scope of the privacy policy document is analyzed according to expressions related to data collection, sharing and storing processes. In this context, findings indicate that the privacy document clearly informs users about the gathered data and how these data are used. In contrast to this finding, the methods being used for data collection processes are not explained in the document. It is also seen that the document states which information will be shared with third parties and the sharing purposes. Accordingly, findings reflect that the data protection measures are slightly presented in the document. On the other hand, the document does not cover how long the gathered data will be stored and its deletion procedures. Although the contact information is provided in help documents, the privacy document does not contain this information.

Evaluations about the privacy policy document of the e-pulse app show that the document is insufficient in terms of scope and structure. The document meets only five (38%) of 13 criteria that are expected to be given in a privacy policy document.

C. Data Sharing and Handling

In the second section of the survey, data sharing and handling functions of the e-pulse system analyzed with 12 questions. These questions are categorized under three titles. These categories are data sharing with third parties, policies, and accessibility.

Findings illustrate that the app is in a very sufficient level in terms of data sharing with third parties. Since the health organizations, mostly hospitals, feed the app with patient transactions in data creation processes, the data handled in third parties is not used in the app. Additionally, the app does not make a request for creating persistent cookies. The third-party tracking cookies blocked by web browsers are not used in the app. Lastly, the privacy policy document strongly emphasizes the conditions related to data sharing and usage conditions with third parties.

Analysis indicates that the e-pulse application provides a secure connection (https) in the web platform and provides access to whole data about the user. It is also seen that the app authenticates the user via e-government account information. Accordingly, users are allowed to modify or delete some of the data such as comments, weight, and size. In contrast, users can not make any changes in their health records. They can only view this data by using the app. It is a remarkable finding that the privacy document partially informs the users about these features. The app also does not provide an explanation of data transmission and storage processes in the privacy document. Findings reveal that the app successfully performs 10 of 12 questions. Findings also demonstrate that one question is partially carried out. In this context, the efficiency of the app in data sharing and handling issues was measured as 87.5%.

D. Privacy Settings and Security

As the third section of the research instrument, privacy settings and security features offered for personal accounts were assessed with 11 questions. In this regard, the authentication process of the app during the login was analyzed. Findings reflect that the app uses a two-factor authentication process and validate users by sending an SMS. Additionally, the app allows users to set which profile information or transaction will be shared with whom.

The app provides five options related to sharing patient transactions with third parties. These options are sharing health data with the family doctor, only the doctor who examines the user, all doctors in the hospital, all doctors employing for the Turkish Ministry of Health or sharing the health data with no one. When the user selects this option, the app asks for approval with SMS. Accordingly, although the user selects "do not share my data with doctors" option, the app allows whole doctors in the hospital where the user made an appointment will see the health data without approval. The related notification is also given under this option. It is a remarkable finding that the privacy policy document does not contain any information about these options, but help documents partially provide these details by giving screenshots.

The app also helps users to make their privacy settings by providing a default setting about sharing health data.

 ISBN: 978-1-61208-759-7

Moreover, users are expected to make their privacy settings in the first use of the app and they are directed to settings panel after the download.

The app allows users to snooze, close or re-open their accounts. In parallel with the findings of the data sharing settings, the privacy policy document does not cover these functions. Users can only learn their rights related to snoozing or closing their accounts via help documents linked on the official web page of the app. Lastly, the app has data validation features and asks users to provide feedback about the misinformation presented in their profile panel. In general, the assessments about privacy settings and security reveal that the app provides many options and features related to privacy and security. It is seen that the technical part of the app meets the basic criteria for privacy and security settings. Although given advantages, documentation of these settings is seen insufficient level especially regarding privacy policy documents. As a result of these insufficiencies, the app performs eight questions completely and it is seen that the requirements in one question are partially carried out. The performance of the app in this part is measured as 70.3%.

E. General Overview

In addition to specific results presented in previous sections of the study, the app was analyzed in terms of general scores obtained according to responses to questions in each section. In this context, the general overview of the app is illustrated in Figure 1 to display obtained percentages of each component, and to compare the levels of each section.

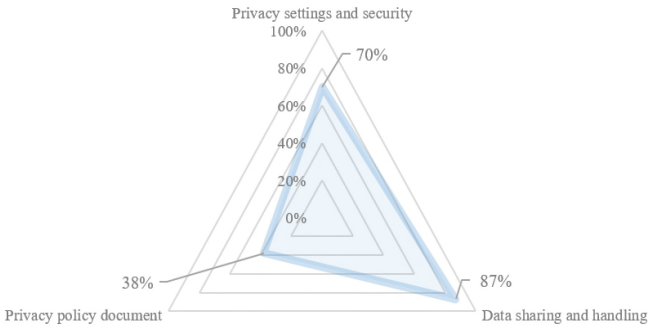

Figure. 1. A general overview of the analyzed components

According to the general situation illustrated in Figure 1, the level of data sharing and handling functions (87%) which are mostly based on the technical processes are higher than the other two sections analyzed in the study. In contrast, the privacy policy document is the weakest component (38%) of the app.

IV. CONCLUSION

The e-Pulse app is an app that is used in Turkey to meet goals expected from mhealth apps such as ensuring that patients have more information about their health information and their participation in treatment decisions. As is in other mhealth apps, processes like patient privacy, security, and privacy of personal data are important for the e-pulse app. Since the app is developed by the Turkish Ministry of Health, all data created in Turkish health institutions are accessible by the app. This situation makes the app's data processes more important. According to the analysis conducted with a checklist developed in this study, it is understood that the app has a privacy, use and copyright agreement. Assessments based on the structure and clarity of the agreement reveal that although the agreement has headings related to the security of personal data, limits of responsibility and copyrights, the provided information under these titles has not been made clear and detailed. It is seen that the processes about data sharing with third parties are expressed in the agreement. In contrast, information about data collection, processes and storage conditions are not expressed. Assessments reflect that the responsibilities during the loss or vulnerability of personal data are not accepted by the app developers. This situation is considered a significant deficiency in the security and confidentiality of the data of the users. Although the application provides users' confidentiality, use, and copyright agreement, the fact that this agreement does not contain detailed information on the confidentiality, security, and information about the protection of patient privacy. These insufficiencies constitute a weakness for the users who need to be clearly informed before using the app. It is clear that there are deficiencies in the documentation for the functions and features related to the privacy and data collection processes of the app. Additionally, evaluations of the application's privacy policy document point out that the document is insufficient in terms of scope and structure. In this context, it is recommended privacy policy document of the app should be improved in terms of data collection, processing and storage issues.

The results presented under the Privacy Settings and Security section of the study reflect that the app provides users five different security options. In this part, users are allowed to select one or more options given by the app. It is remarkable that there is a description given under one of these options. It is located under the "no physician needs to see my data (with SMS code or password required by this option is checked)" option. The description is "If you check this box and make an appointment with the Central Patient Appointment System, all physicians in the relevant hospital will be able to access your health records without obtaining further approval during that examination day." Although the user checks "the physician is not allowed to see the user's data" option, all physicians in the hospital could see the records on the appointment day. This situation conflicts with patient privacy that is also emphasized in the Patient Right Regulation in Turkey [17]. The 16th article of this regulation is "The patient may examine the file and records, which have information on his/her health status, directly or through his/her representative or legal representative and take a copy. These records can only be seen by those directly involved in the treatment of the patient". In addition, the app's privacy policy document does not provide detailed information about

 ISBN: 978-1-61208-759-7

these sharing options. On the other hand, two-factor authentication function and user feedback features of the app were evaluated as positive security and validation methods in the study.

It is understood from the results of the analysis conducted on the e-pulse that the app has deficiencies in the scope of the privacy, use and copyright agreement and this document needs to be improved regarding this issue. In this respect, the application developers are recommended to inform the users about the data collection, storage, and distribution in the privacy policy of the app. As another suggestion, the policy developers of the app are recommended to ensure the readability and intelligibility of the policy documents. Lastly, as stated in the literature, the lack of standardized format and terminological unity in these policies are considered as one of the weaknesses in this topic. In this regard, publications like standards and guidelines that can be published by authority institutions are seen as one of the major steps.

REFERENCES

[1] M. Rowan and J. Dehlinger, "A Privacy Policy Comparison of Health and Fitness Related Mobile Applications," Procedia Computer Science, vol. 37, pp. 348-355, 2014, doi:10.1016/j.procs.2014.08.051.

[2] G. Catan, R. Espanha, R. Veloso Mendes, O. Toren, and D. Chinitz, "The Impact of eHealth and mHealth on doctor behavior and patient involvement: an Israeli and Portuguese comparative approach," Stud Health Technol Inform. vol. 210, pp. 813-817, 2015.

[3] A.M. McDonald and L.F. Cranor, "The Cost of Reading Privacy Policies," vol. 4:3, pp. 543-568, 2008.

[4] D. Ding, M. Conti, and A. Solanas, "A smart health application and its related privacy issues," 2016 Smart City Security and Privacy Workshop (SCSP-W), pp. 1-5, 2016, doi:10.1109/SCSPW.2016.7509558.

[5] L. Parker et al. "A health app developer's guide to law and policy: a multi-sector policy analysis," BMC Medical Informatics and Decision Making. vol. 17, pp.1-13, 2017, doi:10.1186/s12911-017-0535-0.

[6] Privacy and Mobile Apps, Office of the Information Commissioner. [Online]. Available from: https://www.oic.qld.gov.au/guidelines/for-government/guidelines-privacy-principles/applying-the-privacy-principles/privacy-and-mobile-apps 2019.03.28.

[7] M. Al Ameen, J. Liu, and K. Kwak, "Security and Privacy Issues in Wireless Sensor Networks for Healthcare Applications," J Med Syst., vol. 36, pp. 93-101, 2012, doi:10.1007/s10916-010-9449-4.

[8] T. Giannetsos, T. Dimitriou, and N.R. Prasad, "People-centric sensing in assistive healthcare: Privacy challenges and directions," Security and Communication Networks, vol. 4, pp. 1295-1307, 2011, doi:10.1002/sec.313.

[9] P. Dadhich, K. Dutta, and M.C. Govil, "Trust Enhanced Authorization for Distributed Systems," International Journal of Scientific & Engineering Research, vol. 2, pp. 1-7, 2011.

[10] C. Lin and V. Varadharajan, MobileTrust: a trust enhanced security architecture for mobile agent systems, International Journal of Information Security. vol.9 (3), pp. 153–178, 2010. doi:10.1007/s10207-009-0098-x.

[11] Z. Yan, Y. Chen, Y. Shen, "PerContRep: A Practical Reputation System For Pervasive Content Services," J Supercomput, vol. 70, pp.1051-1074, 2014, doi:10.1007/s11227-014-1116-y.

[12] App Review - App Store - Apple Developer. [Online]. Available from https://developer.apple.com/app-store/review/ 2019.03.28.

[13] GSMA Public Policy | Privacy Design Guidelines for Mobile Application Development. [Online]. Available from https://www.gsma.com/publicpolicy/resources/privacy-design-guidelines-mobile-application-development 2019.03.28.

[14] Medical devices: software applications (apps). [Online]. Available from https://www.gov.uk/government/publications/medical-devices-software-applications-apps 2019.03.28.

[15] Office of the A.I. Commissioner, Mobile privacy: a better practice guide for mobile app developers - Office of the Australian Information Commissioner (OAIC). [Online]. Available from https://www.oaic.gov.au/agencies-and-organisations/guides/guide-for-mobile-app-developers 2019.03.28.

[16] A. Sunyaev, T. Dehling, P. Taylor, K. Mandl, "Availability and Quality of Mobile Health App Privacy Policies," Journal of the American Medical Informatics Association, vol. 22, pp. e22-e28, 2015, doi:10.1136/amiajnl-2013-002605.

[17] Patient Rights Guide, Legislation for Physicians and Managers of Medical Chamber. [Online]. Available from http://www.ttb.org.tr/mevzuat/index.php?option=com_content&view=article&id=984:hasta&catid=26:etik&Itemid=65 2019.05.06.

 ISBN: 978-1-61208-759-7