Assessing the Privacy Policies in Mobile Personal Health Records

Belén Cruz Zapata, Antonio Hernández Niñirola, José Luis Fernández-Alemán, Ambrosio Toval

Abstract—**The huge increase in the number and use of smartphones and tablets has led health service providers to take an interest in mHealth. Popular mobile app markets like Apple App Store or Google Play contain thousands of health applications. Although mobile personal health records (mPHRs) have a number of benefits, important challenges appear in the form of adoption barriers. Security and privacy have been identified as part of these barriers and should be addressed. This paper analyzes and assesses a total of 24 free mPHRs for Android and iOS. Characteristics regarding privacy and security were extracted from the HIPAA. The results show important differences in both the mPHRs and the characteristics analyzed. A questionnaire containing six questions concerning privacy policies was defined. Our questionnaire may assist developers and stakeholders to evaluate the security and privacy of their mPHRs.**

I. Introduction

Predictions made by the Cisco Global mobile Data Traffic Forecast of 2013 suggest that by 2017 there will be around 1.4 mobile devices per capita throughout the world [1]. This huge evolution of mobile devices has also led to an increase in the use and development of mobile applications. The Mobile Health Market Report for 2013-2017 estimates that over 500 million people will be using mobile healthcare apps by 2015 [2].

Patients are using online search engines to find health related information [3]. Five percent of searches in Google are health related [4] and the use of the Internet to access medical information is known as eHealth [5]. Health professionals recommend that patients keep records containing their information [6][7]. Personal health records (PHR) are applications that allow an individual to access, manage and share his or her information [8]. Although PHRs are available for PCs, the web or USB, patients are searching for more usable and portable means to access their medical information [9]. The medical practice supported by mobile devices is known as mHealth [10], while mobile PHRs are known as mPHRs and allow patients to access their medical information in any place at any time [9]. Although patients are willing to use mPHRs, their quality-in-use rates are low. The barriers to PHR adoption have been identified as organizational boundaries, cultural issues and usability, along with legal concerns and privacy [11]–[14].

Belén Cruz Zapata (b.cruzzapata@um.es), Antonio Hernández Niñirola (antonio.hernandez5@um.es), José Luis Fernández-Alemán(aleman@um.es) and AmbrosioToval(atoval@um.es), are with Department of Informatics and Systems, School of Computer Science, University of Murcia, Murcia, Spain.

The Health Insurance Portability and Accountability Act (HIPAA), which appeared in 1996, proposes general guidelines to enforce the privacy and protection of private medical information. Those entities that develop PHRs under the HIPAA are required by law to safeguard their patients' information, thus increasing customer confidence in their products.

This paper presents an evaluation of a total of 24 free mPHRs for Android and iOS using a questionnaire containing six questions based on the HIPAA and adapted to mobile apps. This paper is organized as follows: Section II explains the research method, while the results obtained are displayed in Section III. Section IV discusses the main findings and presents the limitations of the study. The conclusions obtained from this research are summarized in Section V.

II. Method

A. Systematic Review and Protocol

The search for mPHRs was addressed by using a method adapted to mobile apps from the well-known systematic literature review (SLR) process [15]. This process used formal methods to ensure the accuracy and impartiality of the search process. The Preferred Reporting Items for Systematic reviews and Meta-Analysis (PRISMA)[16] quality reporting guidelines were also followed. The complete method for the systematic review was developed before beginning the search process and includes eligibility criteria, information sources and describes the selection and data collection processes.

B. Eligibility Criteria

The following inclusion criteria (IC) were used. Meeting all the inclusion criteria was mandatory for an mPHR to be selected:

- IC1: mPHRs in the Health category that were not focused on a specific illness or health condition.
- IC2: mPHRs that were free.
- IC3: mPHRs updated after the 1st of January of 2013.

The following exclusion criteria (EC) were applied to the mPHRs that met the ICs. For an mPHR to be selected it could not meet any of the EC:

- EC1: mPHRs that had installation or runtime errors that do not allow the app to be properly examined.
- EC2: mPHRs that completely depended on an external service and could not be evaluated as a single mobile app (full-tethered mPHRs).

C. Information Sources

The sources selected were the following two app repositories: Apple *App Store* and *Google Play*. These are the

978-1-4244-7929-0/14/$26.00 ©2014 IEEE

two most popular app markets and are leaders in both the number of apps available and downloads. With regard to medical apps, both markets also have an important health category, with around 20,000 medical apps in Apple *App Store* and 8,000 medical apps in *Google Play* [17].

D. Selection of mPHRs

The mPHR selection process was organized in five phases:

1) The search for apps from Apple *App Store* and *Google Play*. The search string ("PHR" OR "personal health record") was obtained using the PICO criteria [18] and adapted to the search engines of each market.
2) Manual exploration of each mPHR found and selection based on the ICs and ECs.
3) Manual exploration of mPHRs, their descriptions in the market and in some cases their websites in order to identify their *Privacy Policies*.
4) Complete reading of each *Privacy Policy* and manual extraction of the security characteristics studied.

E. Data Collection Process

Data collection was approached using a data extraction spreadsheet. Each mPHR was evaluated independently by two of the authors. Disagreements were resolved with discussions between the two authors who were involved in the review of the mPHRs.

G. Quality Assessment

The evaluation of the mPHRs was performed through the use of a questionnaire defined by the authors. The questionnaire criteria were extracted from the HIPAA Privacy Rule and based on the principles analyzed by a previous study that reviews the Privacy Policies of web PHRs [14]. The questionnaire was composed of six quality assessment questions that were applied to each mPHR:

- QA1 Can the Privacy Policy be easily accessed?: Y (Yes), the Privacy Policy is available in the application; P (Partially), the Privacy Policy is available in the app description or on the developer's website; N (No), the Privacy Policy is not available.
- QA2 Are changes to the Privacy Policy notified?: Y (Yes), changes to the Privacy Policy are notified the first time the app is used after the changes are made; P (Partially), the changes are not notified. Instead, an update with date on the Privacy Policy is performed; N (No), the changes are not notified.
- QA3 Does the mPHR include a strong authentication mechanism?: Y (Yes), the authentication procedure is based on two or more of the following elements: (i) something the user knows, (ii) something the user possesses and (iii) something the user is; P (Partially), the authentication procedure is based on one of the aforementioned elements; N (No), there is no authentication.
- QA4 Are the data encrypted?: Y (Yes), the data are encrypted in all scenarios; P (Partially) depending on which data it is encrypted or unencrypted; N (No) the data is fully stored and transferred unencrypted.
- QA5 Does the mPHR follow any security standards or laws?: Y (Yes), the mPHR fully complies with both a security standard and a law; P (Partially), the mPHR complies with a security law; N (No), the mPHR does not comply with any security standards or laws.
- QA6 Does the mPHR allow multiple users, and if so, can access be granted and revoked?: Y (Yes), the mPHR allows multiple users and the owner of the data can grant access to and revoke it from other users; P (Partially), the mPHR allows multiple users but they cannot access any other data but their own; N (No), the mPHR only supports a single user.

The scoring procedure was Y (Yes) = 1, P (Partially) = 0.5 and N (No) = 0. The evaluation was performed independently by two authors. Discrepancies were resolved with discussions between the two authors.

III. RESULTS

A. Selection of mPHRs

The initial search phase obtained a set of 203 candidate apps. After applying the ICs, 35 mPHRs were selected. These 35 mPHRs were reduced to the final amount of the 24 selected for the review after applying the ECs. Fig. 1 shows a PRISMA flow diagram that summarizes this process.

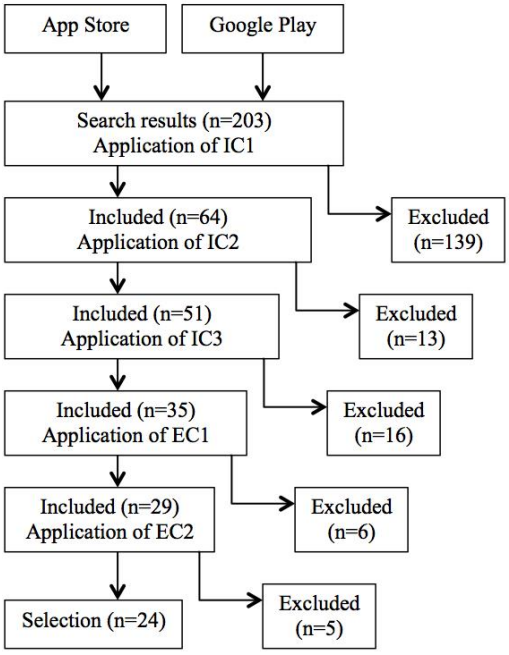

Figure 1. PRISMA Flow Diagram.

B. Quality Evaluation of mPHRs

The results for each app are shown in Table I. The results of the quality assessment show that two apps scored 0, two apps scored 1, two apps scored 1.5 and eight apps scored 2.5. Ten apps obtained more than half of the maximum score: two apps scored 3 and eight apps scored 3.5. None of the apps scores more than 3.5 points out of 6.

TABLE I. QUALITY EVALUATION OF MPHRS. OS=OPERATING SYSTEM (ANDROD/IOS), TS= TOTAL SCORE

mPHR	OS	Quality assessment question						TS
		1	2	3	4	5	6	
CareFlowPHR	And	N	N	P	N	N	P	1
CareSync	iOS	Y	P	P	P	N	Y	3,5
EasyMed Medical Passport	iOS	P	N	P	N	N	P	1,5
EasyMed Medical Passport	And	P	N	P	N	N	P	1,5
Health Companion	iOS	Y	P	P	Y	N	P	3,5
Health suite	And	Y	N	N	N	N	N	1
Health2me	iOS	Y	P	P	N	N	P	2,5
Health2me	And	Y	P	P	N	N	P	2,5
HealthStylus	iOS	Y	N	P	P	N	P	2,5
HealthStylus	And	Y	N	P	P	N	P	2,5
iBlueButton	iOS	Y	P	P	Y	N	N	3
iTriage Health	And	Y	P	P	N	P	P	3
iTriage Health	iOS	Y	P	P	N	P	P	3
LifeCard Health Record	iOS	Y	Y	P	P	P	P	4
MTBC PHR	And	Y	P	P	Y	N	P	3,5
MTBC PHR	iOS	Y	P	P	Y	N	P	3,5
My Health Diary	And	Y	P	P	P	N	P	3
MyClinicNotes	iOS	Y	P	P	Y	P	P	4
MyMx Personal H. R.	iOS	Y	P	N	Y	P	N	3
MyWellnessApp	iOS	N	N	N	N	N	N	0
OnPatient Medical Record	And	Y	P	P	N	P	P	3
OnPatient Personal H. R.	iOS	Y	P	P	N	P	P	3
Personal Health Record Lte	iOS	N	N	N	N	N	N	0
Track My Medical Records	And	P	N	P	Y	N	P	2,5

IV. DISCUSSION

A. What is the quality of the mPHRs studied based on their Privacy Policies?

The results show the scores of each mPHR when assessed using the six QA questions described in Section II-G. Each QA and its results will be analyzed in this section:

1) *Can the Privacy Policy be easily accessed?:* Eighteen of the mPHRs allow the user to access the Privacy Policy from within the app. Three apps do not have a Privacy Policy and three apps include the Privacy Policy on the developer's website. The majority of the mPHRs included (87%) meet this requirement at least partially.

2) Are changes to the Privacy Policy notified?: Only one mPHR, *LifeCard Health Record,* notifies the user when the Privacy Policy changes, and only if the user visits the website. Fourteen applications provide a manual indication of the date of the changes to the Privacy Policy but users are not notified. Users of the other nine mPHRs (37%) cannot use tools supplied by the developer to verify whether the Privacy Policy has changed.

3) Does the mPHR include a strong authentication mechanism?: In order to avoid unauthorized access to sensitive medical information, an authentication mechanism is encouraged. However, none of the mPHRs studied included a 2-phase authentication protocol. The most widespread authentication mechanism was a combination of something the user knows: a username and a password. Only four mPHRs do not include an authentication system and rely on the smartphone features to grant user access.

4) Are the data encrypted?: Seven mPHRs (29%) encrypt their data both while stored and while being transferred. Although specific encryption techniques have been designed for PHRs owing to their particular sensitivity [19], 50% of the mPHRs studied do not encrypt the data according to their privacy policies.

5) Does the mPHR follow any security standard?: This QA question achieved the lowest level of compliance. The 24 mPHRs studied do not comply with any standards. However, some apps claim that they comply with the law. Only two apps, by the same developer (*OnPatient PHR* for Android and iOS) indicate that they comply with both the HIPAA and the Health Information Technology for Economic and Clinical Health (HITECH) Act [20]. In addition, *LifeCard Health Record* and *MyMx PHR* comply with Australian laws while *iTriage Health* for Android and iOS and *MyClinicNotes* comply with US laws.

6) Does the mPHR allow multiple users, and if so, can access be granted and revoked?: Only *CareSync* for iOS includes a multiuser functionality that allows users to grant and revoke access to other users. Most mPHRs (75%) allow different users but they can only access their own information.

B. How do results differ between mPHRs for Android or iOS?

Fig. 2 shows the average score per question for Android and iOS apps. The biggest differences can be observed in Questions 2 and 4, in which the iOS average score is higher than the Android average score for both questions. The contrast in Question 2, which concerns the notification of changes to the Privacy Policy, is derived from the fact that *LifeCard Health Record* for iOS is the only mPHR that obtains the highest score in this question. The inequality in Question 4, which concerns data encryption, agrees with some reports that classify the iOS implementation of encryption as having good protection and the Android implementation as having little protection [21][22]. With regard to the remaining questions, no significant discrepancies can be found. The global average score for each system is 0.39 out of 1 for Android and 0.44 out of 1 for iOS. Both systems score similarly and less than half of the maximum score.

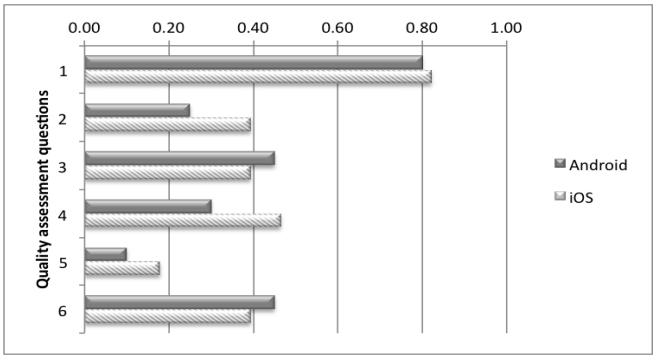

Figure 2. Average score by Operating System

C. Limitations of the study

Although this study was planned and performed with the

aim of attaining the maximum possible objectivity and accuracy, there are some threats to validity of the process. The search process was manual and the search string used may have excluded relevant apps. This threat was mitigated by utilizing the PICO criteria, thus resulting in a simple yet effective search string. The QA questions were extracted from the HIPAA act. Relevant information may have been overlooked which could have affected the evaluation process, thus threatening the conclusion validity. The data extraction was performed by two independent authors in order to mitigate this threat.

V. CONCLUSIONS

Mobile PHRs have a favorable prospective in health technology. One of their main adoption barriers is security and privacy. This paper has presented a questionnaire containing six questions in order to analyze the privacy policy of 24 mPHRs for Android and iOS systems. The questionnaire may also be of use to developers when assessing the privacy of their future mPHRs. Our findings in this study show that no mPHR scores more than 3.5 points out of a maximum of 6. The best way in which to improve mPHRs is to comply with a health care privacy law like HIPAA. Providing a Privacy Policy in mPHRs should be mandatory and renewing the content and structure of the privacy policies is recommended. New authentication methods should be proposed. Users are concerned about their privacy but at the same time search for simpler authentication mechanisms such as biometric techniques [23]. Threat modeling techniques can be used to discover the security and privacy weaknesses of a mobile PHRs [24]. Cross-referenced taxonomy can also be applied to ensure that mobile PHRs comply with HIPAA and HITECH to avoid penalties and lost reputation [25]. As future work, we plan to study how the low quality in Privacy Policies shown in our results may influence mPHR adoption. We also plan to evaluate the privacy policies of the mobile PHRs as regards the information that is stored in the cloud. Cloud services increment the security and privacy requirements [26][27].

ACKNOWLEDGMENT

This research is part of the GEODAS-REQ project (TIN2012-37493-C03-02) financed by both the Spanish Ministry of Economy and Competitiveness and European FEDER funds.

REFERENCES

[1]"Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2012–2017." [Online]. Available: http://www.cisco.com/en/US/solutions/collateral/ns341/ns525/ns537/ns705/ns827/white_paper_c11-520862.html. [Accessed: 17-Oct-2013].

[2]R.-G. Jahns and P. Houck, "Mobile Health Market Report 2013-2017," 2013. [Online]. Available: http://www.research2guidance.com/shop/index.php/mobile-health-trends-and-figures-2013-2017. [Accessed: 23-Nov-2013].

[3]T. H. Van De Belt, L. J. Engelen, S. A. Berben, and L. Schoonhoven, "Definition of Health 2.0 and Medicine 2.0: A Systematic Review," *J. Med. Internet Res.*, vol. 12, no. 2, Jun. 2010.

[4]G. Eysenbach and C. Köhler, "Health-related searches on the Internet," *JAMA J. Am. Med. Assoc.*, vol. 291, no. 24, p. 2946, Jun. 2004.

[5]H. Oh, C. Rizo, M. Enkin, and A. Jadad, "What is eHealth (3): a systematic review of published definitions," *J. Med. Internet Res.*, vol. 7, no. 1, p. e1, 2005.

[6]J. L. Fernández Alemán, I. Hernández, and A. B. Sánchez García, "Encuesta de opinión sobre el uso de historias personales de salud en la Región de Murcia," *Gac. Sanit.*, vol. 27, no. 5, pp. 454–458, Oct. 2013.

[7]N. Huba and Y. Zhang, "Designing patient-centered personal health records (PHRs): health care professionals' perspective on patient-generated data," *J. Med. Syst.*, vol. 36, no. 6, pp. 3893–3905, Dec. 2012.

[8]J. L. Fernández-Alemán, C. L. Seva-Llor, A. Toval, S. Ouhbi, and L. Fernández-Luque, "Free Web-based Personal Health Records: An Analysis of Functionality," *J. Med. Syst.*, vol. 37, no. 6, pp. 1–16, Dec. 2013.

[9]H. Kharrazi, R. Chisholm, D. VanNasdale, and B. Thompson, "Mobile personal health records: An evaluation of features and functionality," *Int. J. Med. Inf.*, vol. 81, no. 9, pp. 579–593, Sep. 2012.

[10] World Health Organization, "mHealth: New horizons for health through mobile technologies," Jun. 2011.

[11] P. C. Tang, J. S. Ash, D. W. Bates, J. M. Overhage, and D. Z. Sands, "Personal Health Records: Definitions, Benefits, and Strategies for Overcoming Barriers to Adoption," *J. Am. Med. Inform. Assoc.*, vol. 13, no. 2, pp. 121–126, Mar. 2006.

[12] L. S. Liu, P. C. Shih, and G. R. Hayes, "Barriers to the Adoption and Use of Personal Health Record Systems," in *Proceedings of the 2011 iConference*, New York, NY, USA, 2011, pp. 363–370.

[13] I. Carrión, J. F. Alemán, and A. Toval, "Personal Health Records: New Means to Safely Handle our Health Data?," *IEEE Computer*, vol. 45, no. 11, pp. 27–33, 2012.

[14] I. CarriónSeñor, J. L. Fernández-Alemán, and A. Toval, "Are Personal Health Records Safe? A Review of Free Web-Accessible Personal Health Record Privacy Policies," *J. Med. Internet Res.*, vol. 14, no. 4, p. e114, Aug. 2012.

[15] P. Brereton, B. A. Kitchenham, D. Budgen, M. Turner, and M. Khalil, "Lessons from applying the systematic literature review process within the software engineering domain," *J. Syst. Softw.*, vol. 80, no. 4, pp. 571–583, Apr. 2007.

[16] D. Moher, A. Liberati, J. Tetzlaff, and D. G. Altman, "Preferred Reporting Items for Systematic Reviews and Meta-Analyses: The PRISMA Statement," *Ann. Intern. Med.*, vol. 151, no. 4, pp. 264–269, Aug. 2009.

[17] T. Aungst, "Apple app store still leads Android in total number of medical apps," *iMedicalApps*, 12-Jul-2013. [Online]. Available: http://www.imedicalapps.com/2013/07/apple-android-medical-app/. [Accessed: 17-Oct-2013].

[18] P. Stone, "Popping the (PICO) question in research and evidence-based practice," *Appl. Nurs.Res.*, vol. 15, no. 3, pp. 197–8, 2002.

[19] L. Ibraimi, M. Asim, and M. Petkovic, "Secure management of personal health records by applying attribute-based encryption," in *2009 6th International Workshop on Wearable Micro and Nano Technologies for Personalized Health (pHealth)*, 2009, pp. 71–74.

[20] D. Blumenthal, "Launching HITECH," *N. Engl. J. Med.*, vol. 362, no. 5, pp. 382–385, 2010.

[21] "Security showdown: iOS 7 vs. Android 4.3 | Head to head," *Softonic*. [Online]. Available: http://features.en.softonic.com/security-showdown-ios-7-vs-android-4-3. [Accessed: 30-Jan-2014].

[22] Carey Nachenberg, "A Window Into Mobile Device Security. Examining the security approaches employed in Apple's iOS and Google's Android.," Symantec, Jun. 2011.

[23] P. Rodrigues and H. Santos, "Health users' perception of biometric authentication technologies," in *Proceedings of the IEEE 26th International Symposium on Computer-Based Medical Systems*, 2013, pp. 320–325.

[24] R. Scandariato, K. Wuyts, and W. Joosen, "A descriptive study of Microsoft's threat modeling technique," *Requir.Eng.*, (In press).

[25] J. C. Maxwell, A. I. Antón, P. Swire, M. Riaz, and C. M. McCraw, "A legal cross-references taxonomy for reasoning about compliance requirements," *Requir. Eng.*, vol. 17, no. 2, pp. 99–115, Jun. 2012.

[26] S. Gritzalis and L. Liu, "Requirements Engineering for Security, Privacy and Services in Cloud Environments," *Requir. Eng.*, vol. 18, no. 4, pp. 297–298, Nov. 2013.

[27] C. Kalloniatis, H. Mouratidis, and S. Islam, "Evaluating cloud deployment scenarios based on security and privacy requirements," *Requir. Eng.*, vol. 18, no. 4, pp. 299–319, Nov. 2013.