33rd Annual International Conference of the IEEE EMBS
Boston, Massachusetts USA, August 30 - September 3, 2011

Assessing the HIPAA Standard in Practice: PHR Privacy Policies

Inmaculada Carrión, José Luis Fernández Alemán and Ambrosio Toval

Abstract— **Health service providers are starting to become interested in providing PHRs (Personal Health Records). With PHRs, access to data is controlled by the patient, and not by the health care provider. Companies such as Google and Microsoft are establishing a leadership position in this emerging market. A number of benefits can be achieved with PHRs, but important challenges related to security and privacy must be addressed. This paper presents a review of the privacy policies of 20 free web-based PHRs. Security and privacy characteristics were extracted and assessed according to the HIPAA standard. The results show a number of important differences in the characteristics analyzed. Some improvements can be made to current PHR privacy policies to enhance the audit and management of access to users' PHRs. A questionnaire has been defined to assist PHR designers in this task.**

I. INTRODUCTION

In recent years, governments around the world have shown an increasing interest in the computerization of health-care records [1]. The growing use of Web 2.0 technologies signifies that patients can access their own health information via tools such as Personal Health Records (PHR). A PHR is"an electronic record of an individual's health information by which the individual controls the access to the information and may have the ability to manage, track, and participate in his or her own health care" [2]. The following benefits can be attained with PHRs [3], [4]: they provide a unified summary of users' entire health histories; they improve physician-patient communication; they are easy to understand and use; they reduce the risk of medical errors.

However, certain barriers prevent users from using PHR systems, despite their benefits. One major barrier is related to the security and privacy of user data [5]. According to Srinivasan, "if consumers doubt the security of online PHR systems, they will not adopt them" [6]. Furthermore, recent research has evaluated the security and privacy of web-based PHRs to verify whether they are usable [7].

In 1996, the Health Insurance Portability and Accountability Act (HIPAA) offered some general guidelines to enforce the protection of private medical information [8]. The entities covered under the HIPAA are required by law to protect the users' information, thus increasing user confidence in these PHRs. However, not all PHR systems are regulated by HIPAA, and consumers should therefore have access to their privacy policy before they start to use these PHRs.

In this paper, the privacy policies of 20 free web-based PHRs are analyzed and assessed according to the HIPAA standard. The remainder of the paper is organized as follows. Section II introduces the research method. Section III offers the main results of the data collected, and the statistical analysis conducted. The main findings are discussed in Section IV. Finally, Section V presents some concluding remarks.

Inmaculada Carrión, José Luis Fernández Alemán and Ambrosio Toval are with Department of Informatics and System, Faculty of Computer Science, University of Murcia, Murcia, Spain mariainmaculada.carrion@um.es, aleman@um.es, atoval@um.es

II. METHOD

A. Systematic review, protocol and registration

The search of PHRs performed in this research has been addressed by a systematic literature review (SLR). This systematic review used formal methods to ensure that both the search and the retrieval process were accurate and impartial. A systematic review is defined as a research technique that attempts to collect all empirical evidence in a particular field, to assess it critically and to obtain conclusions that summarize the research. The objective of an SLR is not only to collect all the empirical evidence of a research question but to support the development of guidelines based on the evidence for professionals. This systematic review followed quality reporting guidelines set out by the Preferred Reporting Items for Systematic reviews and Meta-Analysis (PRISMA) group [9]. A review protocol describing each step of the systematic review, including eligibility criteria, was therefore developed before beginning the search for literature and the data extraction. This protocol was reviewed and approved by A. Toval.

B. Eligibility Criteria

The following inclusion criteria were used:

- *IC1*. PHRs with web-based format
- *IC2*. PHRs which were free
- *IC3*. PHRs with a document called Privacy Policy

C. Information Sources

The PHRs were published on the *myPHR* web site. This web site was created by the American Health Information Management Association (AHIMA) and contains information relating to the use and the creation of PHRs. The search was completed by reading articles extracted from Medline, ACM Digital Library, IEEE Digital Library and Science@Direct databases, and was run between February and March 2011.

D. PHR Selection

The PHR selection was organized in the following six phases:

1) The search for publications from electronic databases related to health and computer science. This phase was

978-1-4244-4122-8/11/$26.00 ©2011 IEEE

performed by using the following search string: ("PHR providers" OR "Microsoft HealthVault' OR "Google Health"), which was adapted to the databases search engines.
2) Exploration of the articles identified in order to discover the names of web-based PHRs.
3) The search for PHRs from the emphmyPHR web site.
4) Exploration of the PHRs found and selection based on eligibility criteria IC1 and IC2.
5) Exploration of the PHR web site identified in order to find the *Privacy Policy* of each one.
6) Complete reading of each of the PHR *Privacy Policies* selected in the previous phase to extract their main security characteristics

The activities defined in the aforementioned phases were carried out independently by I. Carrión and J. L. Fernández. Any discrepancies were resolved by a third member of the team, A. Toval.

E. Data Collection Process

Data collection was carried out by using a data extraction form. Each PHR was assessed by one of the authors of the work presented herein, who read the full text of its Privacy Policy. Therefore, only one reviewer extracted data, while another checked it. Any disagreements were resolved through a discussion between the two authors who had reviewed the PHR.

F. Data Items

We designed a template with the data that should be extracted from each PHR. These features were grouped into three categories:

- *General*. Link of the PHR.
- *Data Management*. Who manages the data in the PHR, what data are managed and what source of information is used.
- *Access Management*. Who manages the access control to the data in the PHR, what types of permission exist and who can receive the access permission.
- *Access Audit*. Is an audit of accesses to data in PHR is performed, and who can see this audit.

G. Quality Assessment

Each PHR was evaluated using certain criteria defined by the authors. The criteria were extracted from the HIPAA Privacy Rule [2] and were applied to the PHR Privacy Policies. The criteria are based on six quality assessment (QA) questions:

QA1 Can the individual access his/her health records with written permission?
QA2 Are the sources of information the individual and health care providers?
QA3 Can the individual control who accesses his/her information?
QA4 Can the individual authorize health care providers to update his/her information?

TABLE I
QUALITY EVALUATION OF PHRS. TS = TOTAL SCORE, 1 = QA1, 2 = QA2, 3 = QA3, ETC.

PHR	1	2	3	4	5	6	TS
Dr. I-Net	P	Y	Y	P	N	N	3
EMRy STICK	Y	P	Y	P	P	P	4
Google Health	Y	Y	Y	Y	P	Y	5.5
HealthButler	Y	P	Y	P	N	N	3
Juniper Health	Y	P	Y	N	P	N	3
Keas	Y	P	U	U	U	N	1.5
MedicAlert	Y	P	Y	P	P	N	3.5
MediCompass	N	N	Y	P	N	N	1.5
MedsFile.com	Y	P	N	N	N	N	1.5
Microsoft Health Vault	Y	P	Y	Y	Y	Y	5.5
MyChart	N	P	P	N	N	P	1.5
My Doclopedia PHR	P	P	Y	P	N	N	2.5
myHealthFolders	Y	P	Y	P	N	P	3.5
My HealtheVet	Y	P	N	N	N	N	1.5
myMediConnect	Y	Y	Y	P	P	N	4
NoMoreClipBoard.com	Y	Y	Y	P	N	P	4
RememberItNow!	Y	P	Y	Y	Y	P	5
Telemedical.com	Y	P	Y	N	P	N	3
VIA	N	U	Y	N	P	N	1.5
ZebraHealth	N	P	U	U	U	N	0.5

QA5 Does the system allow the individual to designate family members or other persons to have access to his/her information?
QA6 Does the PHR provide the individual with the ability to view a log of who has accessed his/her PHR?

The questions were scored as follows:

- QA1: Y (Yes), the individual can access all of his/her health records with read and written permission; P (Partly), the individual can access all of his/her health records with a read permission and he/she can access part of his/her health records with written permission; N (No) the individual can only access all of his/her health records with a read permission.
- QA2: Y, the information is obtained from the individual and health care providers; P, the information is obtained from the individual or from health care providers; N, the information is obtained from a different source.
- QA3: Y, the individual can grant and revoke the access to his/her information; P, the individual can request to grant access to his/her information to someone, but the system is not required to agree to the individual's request in most cases; N, the individual cannot explicitly grant/revoke access to his/her information in the PHR.
- QA4: Y, the individual can authorize health care providers to view and update his/her information; P, the individual can authorize health care providers to view his/her information; N, the individual cannot authorize health care providers to either view or update his/her information.
- QA5: Y, the individual can share his/her information with friends and his/her family members; P, the individual can share his/her information with other system users; N, the individual cannot share his/her information with friends, his/her family members or other system

users.

- QA6: Y, the individual can see who has accessed his/her data and with what aim; P, the individual can see who has accessed his/her data; N, the individual cannot see who has accessed his/her data.

The scoring procedure was Y = 1, P = 0.5, N = 0, or Unknown = 0 (i.e. the information is not specified). I. Carrión assessed 20 PHRs, and allocated 10 PHRs to each of the other authors of this study for their independent assessment. When there was a disagreement, the issues were discussed until an agreement was reached.

III. RESULTS

A. Study Selection

A total of 20 PHRs were identified in the review. The search of databases and the *myPHR* web site provided a total of 51 different PHRs, although 2 were discarded because they did not meet the criterion of IC1. Another 21 PHRs were then discarded because they clearly did not meet the criterion of IC2 and, finally, 3 PHRs were discarded because they did not meet the criterion of IC3. The Privacy Policies of the remaining 25 PHRs were examined and 5 of these were discarded because they were not patient-centered PHRs. Fig. 1 shows a PRISMA flow diagram that summarizes this process.

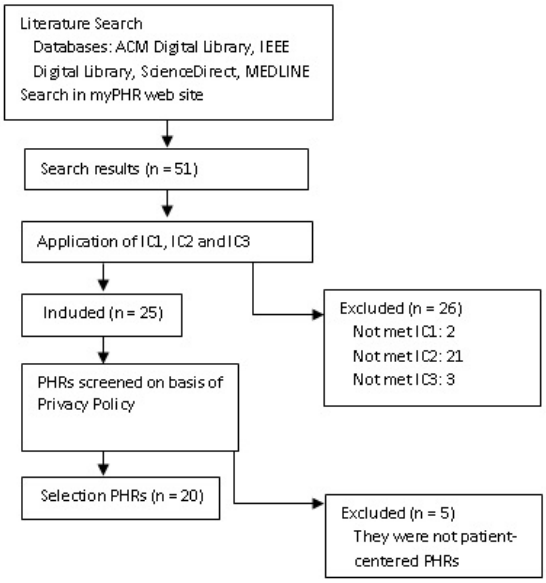

Fig. 1. PRISMA Flow Diagram

B. Quality Evaluation of PHRs

The Privacy Policy of each PHR included in the review was assessed by using the criteria extracted from the HIPAA Privacy Rule (see Section II-G). The score for each PHR is shown in Table I. The results of the quality analysis show that only one PHR scored less than 1 [10]. Six PHRs scored 1.5 [11]–[16], one PHR scored 2.5 [17], four PHRs scored 3 [18]–[21], two PHRs scored 3.5 [22], [23], three PHRs scored 4 [24]–[26], one PHR scored 5 [27] and two PHRs scored 5.5 [28], [29].

TABLE II
AVERAGE QUALITY SCORES FOR PHRS BY USE OF STANDARDS

	Not use standards	Use standards
Number of PHRs	12	8
Mean quality score	3.33	2.375
Standard deviation of quality score	1.18	1.66

C. Quality factors

The relationship between the quality score for a PHR and the use or non use of the standards for PHRs was investigated. The PHRs reviewed are based on HIPAA or HONcode standard or both. The average quality scores for PHRs grouped by the use or non use of the standards is shown in Table II. Note that the number of PHRs which do not support standards is higher than those which do. The average quality score is higher in PHRs which are not based on standards.

IV. DISCUSSION

In this section the answers to our research questions are discussed.

A. What functionality has been implemented in the PHRs?

In order to verify this question, six requirements were defined. These requirements are consistent with the QA questions described in Section II-G. This research question was therefore broken down into the six items described below:

1) Can the individual access his/her health records with written permission?: Fourteen of the PHRs included in the review (70%) allow individuals to access their PHRs with written permission. This shows that the majority of the PHRs reviewed meet this requirement.

2) Are the sources of information the individual and the health care providers?: Only four of the PHRs analyzed (20%) meet this requirement. In the majority of the PHRs reviewed (70%), the source of information is either the individual or the health care providers, but not both.

3) Can the individual control who accesses his/her information?: Fifteen of the PHRs included (75%) allow individuals to control who has access to their information. This shows that this requirement is met by the majority of the PHRs reviewed.

4) Can the individual authorize health care providers to update his/her information?: Only three of the PHRs analyzed (15%) meet this requirement. In the majority of the PHRs reviewed (45%), only the health care provider can see the individual's information.

5) Does the system allow the individual to designate family members or other people to have access to his/her information?: Only two of the PHRs included (10%) meet this requirement. The majority of the PHRs analyzed (45%) do not allow the individual to share his/her information with friends, family members or other system users.

6) Does the PHR provide the individual with the ability to view a log of who has accessed his/her PHR?: Only two of the PHRs reviewed (10%) meet this requirement. The majority of the PHRs analyzed (65%) do not allow the individual to see who has accessed his/her data.

Our requirements are not being met by the PHRs analyzed. Only the first and third requirements appear to be among the main trends of the current PHRs.

B. Final Evaluation

As shown, the average quality of PHRs which are not based on standards is higher than that of standard-based PHRs. Note that in this study only a part of the HIPAA has been taken into account and, although these PHRs do not comply with the HIPAA, some of them have been based on it to develop their PHR systems, such as Google Health and Microsoft HealthVault. Moreover, this type of PHRs needs to have privacy policies of a higher quality if users are to believe that their data are protected in these systems.

Finally, the standard-based PHRs have privacy policies of a lower quality because they indicate that they are based on standards and this ensures that users' data are protected. However, this may not be sufficient for some users, and the privacy policies of these PHRs should therefore be improved.

C. Limitations

Our study may have several limitations: (1) The search was organized as a manual search process of several databases. The search string may not have included words that would have selected other relevant PHRs. (2) The authors have not included those PHRs which had a defined Privacy Policy, but which could not be found on the PHR's web site. (3) One researcher extracted the data from each PHR and another checked them. The reviewers may have omitted data which was relevant to this study.

V. CONCLUSION

After defining certain requirements that we considered to be part of the basic functionality of a PHR, we have discovered that five of the PHRs analyzed (25%) comply with them either totally or partially. This percentage is very small if we consider that our requirements catalog consists of six requirements.

The designers of PHRs or the designers of their Privacy Policies consider the individual's permissions and the sources of information in their PHRs, but other characteristics such as who controls the access to the information in the PHR are not considered, at least in the Privacy Policies of PHRs. Both the PHRs and their Privacy Policies should therefore be improved, particulary the latter because the Privacy Policy is a very important document which the system users should employ to discover how their personal information is being dealt with. Some improvements proposed are to include the answers to the following questions in the Privacy Policy: *Who manages the data in the PHR?*, *What data are managed?*, *What is the source of information used?*, *Who manages the access control to the data in the PHR?*, *What types of permission exist?*, *Who can receive access permission?*, *Is an audit of access to data in the PHR performed?*, and *Who can see this audit?*.

ACKNOWLEDGMENT

This work has been partially financed by the Spanish Ministry of Science and Technology, project PANGEA, TIN2009-13718-C02-02.

REFERENCES

[1] S. P. Sood, S. N. Nwabueze, V. W. A. Mbarika, N. Prakash, S. Chatterjee, P. Ray, and S. Mishra, *Electronic Medical Records: A Review Comparing the Challenges in Developed and Developing Countries*, ser. HICSS '08. Washington, DC, USA: IEEE Computer Society, 2008. [Online]. Available: http://dx.doi.org/10.1109/HICSS.2008.141

[2] Personal Health Records and the HIPAA Privacy Rule. [Online]. Available: http://www.hhs.gov/ocr/privacy/hipaa/understanding/special/healthit/phrs.pdf

[3] myMediConnect Personal Health Records. [Online]. Available: http://www.mymediconnect.net/phr.php

[4] J. Bonander and S. Gates, "Public health in an era of Personal Health Records: Opportunities for innovation and new partnerships," *Journal of Medical Internet Research*, vol. 12, no. 3, p. e33, 2010.

[5] 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*, ACM, Ed., New York, NY, USA, 2011, pp. 363–370.

[6] A. Srinivasan, "Keeping online personal records private: security and privacy considerations for web-based PHR systems," *Journal of AHIMA*, vol. 77, no. 1, pp. 62–63, 68, 2006.

[7] I. Carrión, J. L. F. Alemán, and A. Toval, "Usable privacy and security in Personal Health Records," in *13th IFIP TC13 Conference on Human-Computer Interaction*, 2011 (accepted for publication).

[8] L. C. Huang, H. C. Chu, L. C. Y., H. C. H., and K. T., "Privacy preservation and information security protection for patients' portable electronic health records." *Computers in Biology and Medicine*, vol. 39, no. 9, pp. 743–750, 2009.

[9] A. Liberati, D. G. Altman, J. Tetzlaff, C. Mulrow, P. C. Gtzsche, J. P. Ioannidis, M. Clarke, P. Devereaux, J. Kleijnen, and D. Moher, "The PRISMA statement for reporting systematic reviews and meta-analyses of studies that evaluate health care interventions: explanation and elaboration," *Journal of Clinical Epidemiology*, vol. 62, no. 10, pp. e1–e34, 2009.

[10] ZebraHealth. [Online]. Available: https://www.zebrahealth.com/

[11] Keas. [Online]. Available: https://www.keas.com/

[12] MediCompass. [Online]. Available: https://www.medicompass.com/mcweb/default.aspx

[13] MedsFile.com. [Online]. Available: http://www.medsfile.com/

[14] MyChart. [Online]. Available: https://www.mychartlink.com/mychart/

[15] My HealtheVet. [Online]. Available: http://www.myhealth.va.gov/

[16] VIA. [Online]. Available: https://www.mivia.org/

[17] My Doclopedia PHR. [Online]. Available: https://www.doclopedia.com/Login.aspx

[18] Dr. I-Net. [Online]. Available: http://www.drinet.com/

[19] HealthButler. [Online]. Available: http://healthbutler.com/

[20] Juniper Health. [Online]. Available: https://juniperhealth.com/

[21] Telemedical.com. [Online]. Available: http://www.telemedical.com/

[22] MedicAlert. [Online]. Available: http://www.medicalert.org/home.html

[23] myHealthFolders. [Online]. Available: https://myhealthfolders.com/

[24] EMRy STICK. [Online]. Available: http://phr.emrystick.com/

[25] myMediConnect. [Online]. Available: http://www.mymediconnect.net/index.php

[26] NoMoreClipBoard.com. [Online]. Available: http://www.nomoreclipboard.com/

[27] RememberItNow! [Online]. Available: http://www.rememberitnow.com/

[28] Google Health. [Online]. Available: www.google.com/health/

[29] Microsofth HealthVault. [Online]. Available: http://www.healthvault.com/personal/index.aspx