Usable privacy and security in Personal Health Records

Inma Carrión, Jose L. Fernández-Alemán, Ambrosio Toval

Department of Informatics and Systems, University of Murcia, Spain
{mariainmaculada.carrion, aleman, atoval}@um.es

Abstract. PHRs (Personal Health Records) store individuals' personal health information. Access to this data is controlled by the patient, rather than by the health care provider. Companies such as Google and Microsoft are establishing a leadership position in this emerging market. In this context, the need for psychological acceptability in privacy and security protection mechanisms is essential. Any privacy and security mechanism must be acceptable from a usability perspective. This paper presents a study of the privacy policies of 22 free web-based PHRs. Security and privacy characteristics have been extracted according to the ISO/TS 13606-4 standard. In general, quite a good level was observed in the characteristics analyzed. Nevertheless, some improvements could be made to current PHR privacy policies to enhance the management of other users' data, the notification of changes to the privacy policy to users and the audit of accesses to users' PHRs.

Keywords: Usable privacy, usable security, PHRs, healthcare.

1 Introduction

In recent years, governments around the world have shown an increasing interest in computerizing health-care records [1]. The growing use of Web 2.0 technologies signifies that patients can now access their own health information via tools such as Personal Health Records (PHRs). The Markle Foundation defines a PHR as "An electronic application through which individuals can access, manage and share their health information, and that of others for whom they are authorized, in a private, secure, and confidential environment" [2]. The following benefits can be attained with PHRs [3][4]: (i) they provide a unified summary of users' entire health histories; (ii) they are easy to understand and use; (iii) 24/7 access to all users' healthcare data from anywhere in the world; (iv) collaborative disease tracking; and (v) continuous communication between patient and physicians.

At present, a number of cutting-edge companies such as Google and Microsoft attempt to deliver healthcare services with their own PHRs: Google Health and Microsoft HealthVault. However, a number of new security and privacy threats hang over patients' health data in this context [5]. Information might be fragmented and accessible from several sites (by visiting different doctors' offices, hospitals, providers, etc). Safety defects in some of these systems could cause the disclosure of information to unauthorized people or companies, and health data therefore need protection against manipulations, unauthorized access and abuses. Data needs careful

protection, thus leading to the necessity for extreme strictness in storage and information exchange activities.
These threats are arguably more challenging than those found in most other industry sectors owing to [6]: (1) the amount of patient health record entries; (2) the number of healthcare personnel and organizations that might come into contact with a patient at any one time; (3) the difficulty involved in classifying the sensibility of a patient record entry; (4) the provision of very rapid appropriate access in a distributed computing environment; (5) the need for reviews of access permissions and for the PHR entries to be rigorously managed.

This research aims to study the privacy and security of PHRs from a usability perspective. The privacy policies of 22 free web-based PHRs were analyzed to extract their main characteristics. Our study on usable privacy and security is classified as a *security feature study*, according to the five-category framework presented by Birge [7]. The remainder of the paper is organized as follows. Section 2 justifies the importance of this research by reviewing the related literature. Section 3 introduces the method used in the experiment: instrumentation, experimental procedure and analysis of characteristics. Section 4 shows the principal results obtained from the data collected. Finally, Section 5 presents some concluding remarks.

2 Related work

In recent years, relevant research has been carried out into PHRs, particularly with regard to the most popular PHRs, Google Health and Microsoft HealthVault. Martino and Ahuja [8] assessed these platforms to highlight those vulnerabilities existing in PHR privacy policy coverage and gaps in privacy policy notification mechanisms. The authors used well-researched evaluation criteria reported in literature [9, 10, 11].

Kotz et al. [12] compare existing privacy frameworks and identify a privacy framework for mobile healthcare and home-care systems. Mohan and Blough [13] propose a framework which supports the need to change the rule and policy combination algorithms dynamically based on contextual information. Williams [14] presents a survey of the research literature related to the security and privacy of personal health information in social networking applications, and provides a snapshot of privacy and security safeguards for social network websites. Huang et al. [15] design a method according to HIPAA guidelines to preserve the privacy and security of patients' portable medical records in portable storage media. Carrión et al. evaluate the privacy policies of 20 PHRs to check that the privacy of patients' data was preserved in accordance with HIPAA guidelines [16]. Sunyaev et al. develop criteria to assess the PHR systems from the users' viewpoint. The criteria were classified into three categories: patient information, personal control and additional services [17]. To illustrate their proposal, these authors applied the criteria to Google Health and Microsoft HealthVault. Sunyaev et al. [18] also performed an evaluation of Google Health API and Microsoft HealthVault API. An evaluation of the ethical, legal, and social issues (ELSI) was presented by Cushman et al. [19], who group this evaluation in four areas: privacy and confidentiality, data security, decision support, and the legal-regulatory regime for health data.

In this work, we analyze 22 free web-based PHRs, including Google Health and Microsoft HealthVault. To the best of our knowledge, no other studies have dealt with the security and privacy features of so many PHRs.

3 Classification Framework

3.1 Instrumentation

The problem of selecting the set of PHRs to be included in the study was confronted by consulting the web site of the American Health Information Management Association (AHIMA): *myPHR*. Its url is *www.myphr.com* and contains large amount of information on the PHRs. To the best of our knowledge, this web site provides the most comprehensive list of PHRs that a user can find, and has also been used to select PHRs in multi-source sampling [20]. It includes a section called "Choose a PHR" which was used to obtain a free web-based PHRs list. At the moment of accessing it on March 2011, a total of 29 free web-based PHRs (specified in Table 1) were retrieved. Note that AHIMA classifies the PHRs according to their format and cost. In this respect, some PHRs have premium accounts, and can thus also be classified as "for purchase".

Table 1. PHRs lists hosted in AHIMA.

Format	Cost	Amount
Web-based	Free	29
Software-based	Free	0
Paper-based	Free	3
Web-based	For Purchase	63
Software-based	For Purchase	1
Paper-based	For Purchase	13

3.2 Experimental procedure

The privacy policy of each PHR selected was reviewed by one author. This review was carried out between February and March 2011. Difficulties were encountered in seeking the PHRs' privacy policy because some of them were not on the PHR home page and others were fragmented in several documents. While the review was conducted, the formulation criteria for the enquiries was carefully discussed and agreed in an attempt to obtain a comparative framework that would be as comprehensive and clear as possible. Moreover, a number of the listed PHRs were not in force, or had no privacy policy or an equivalent document. In conclusion, the original amount of PHRs for participation (29) was reduced to 22.
The ISO/TS 13606-4 [6] is a Technical Specification (TS) which provides a basic framework that can be used as a minimum specification for an EHR (Electronic

Health Records) access policy, and a generic representation for the communication of policy information. We have adopted ISO/TS 13606-4 as the basis of a classification framework for the evaluation of the set of relevant PHR features. According to the ISO/TS 13606-4: (P1) “health records should be created, processed and managed in ways that guarantee the confidentiality of their contents and legitimate control by patients in how they are used”; (P2) “the subject of care has the right to play a pivotal role in decisions on the content and distribution of his or her electronic health record, as well as rights to be informed of its contents”; (P3) “the communication of health record information to third parties should take place only with patient consent”. A number of PHR security and privacy features have been defined according to these principles.

3.3 Analysis of Characteristics

Nine security characteristics were defined to analyze the PHRs: Privacy policy location, Data source, Data managed, Access management, Access audit, Data accessed without the user's permission, Security measures, Changes in privacy policy and Standards:

Privacy Policy Location. This characteristic is related to the question *Where is the Privacy Policy on the PHR web site?* PHRs should provide a Privacy Policy which describes how users' data are used in order for users to be informed. The Privacy Policy should be easily accessible by users. The difficulty of Privacy Policy access is assessed by counting the number of links clicked. The values that this characteristic may take are:

0. The Privacy Policy is not visible or not accessible.
1. The Privacy Policy is accessed by clicking one link.
2. The Privacy Policy is accessed by clicking two or more links.

Data Source. This characteristic is related to the question *Where do users’ PHR data proceed from?* Generally, the user is his/her data source, but there are PHRs which do not only use this source. Some contact the users' healthcare providers, others allow other users and different programs to enter users' data and others use self-monitoring devices to obtain users' data. The values that this characteristic may take are:

0. Not indicated.
1. User.
2. User healthcare provider.
3. User and his/her healthcare providers.
4. User, other authorized users and other services/programs.
5. Self-monitoring devices connected with the user.

Data Managed. This characteristic is related to the question *Who do the data managed by the users belong to?* The users can manage their own data, but they can sometimes manage other users' data, such as that of their family. The values that this characteristic may take are:

0. Not indicated.
1. Data user.
2. Data user and his/her family data.

Access management. This characteristic is related to the question *Who can obtain access granted by the users?* The users decide who can access their PHR data. The PHR systems analyzed allow access to be given to different roles. The values that this characteristic may take are:

0. Not indicated.
1. Other users and services/programs.
2. Healthcare professionals.
3. Other users.
4. Other users, healthcare professionals and services/programs.

Access audit. This characteristic is related to the question *Can users see an audit of accesses to their PHRs?* The values that this characteristic may take are:

0. No.
1. Yes.

Data accessed without the user's permission. This characteristic is related to the question *What data are accessed without the user's explicit consent?* The PHR systems typically access certain data related to the users in order to verify that everything is correct. The values that this characteristic may take are:

0. Not indicated.
1. Information related to the accesses.
2. De-identified user information.
3. Information related to the accesses and de-identified user information.
4. Information related to the accesses and identified user information.

Security measures. This characteristic is related to the question *What security measures are used in PHR systems?* There are two types of security measures: physical measures and electronic measures. The physical security measures are related to the protection of the servers in which the data are stored. The electronic security measures are related to how stored and transmitted data are protected, for example, by using a Secure Sockets Layer (SSL) scheme. The values that this characteristic may take are:

0. Not indicated.
1. Physical security measures.
2. Electronic security measures.
3. Physical security measures and electronic security measures.

Changes in Privacy Policy. This characteristic is related to the question *Are changes in privacy policy notified to users?* Changes in Privacy Policy should be notified to users in order to make them aware of how their data are managed by the PHR system. The values that this characteristic may take are:

0. Not indicated.
1. Changes are notified to users.
2. Changes are announced on home page.
3. Changes are notified to users and changes are announced on home page.
4. Changes may not be notified.

Standards. This characteristic is related to the question *Are PHR systems based on privacy and security standards?* The PHR systems analyzed use or are based on two standards: the *Health Insurance Portability and Accountability Act* (HIPAA) [21] and the *Health On the Net Code of Conduct* (HONcode) [22]. The values that this characteristic may take are:

0. Not indicated.
1. HIPAA is mentioned.
2. System is covered by HONcode.
3. HIPAA is mentioned and system is covered by HONcode.

4 Results

Table 2 shows the results obtained for each PHR system included in the review. For example, Google Health takes the value 1 (according to the numbering in Section 3) for the PL characteristic. The scores were calculated according to the security and privacy characteristics of the PHRs. The following variables are considered in this study: The security level was quantified by employing the characteristics: Access audit and Security measures. The privacy level was quantified by using the characteristics: Privacy policy location, Cookies, Changes in privacy policy and Data accessed without the user's permission. Fig. 1 shows these scores as two overlapping histograms. In general, quite a good level can be observed in the characteristics analyzed. Nevertheless, some improvements could be made to current PHR privacy policies to enhance specific capabilities such as: the management of other users' data, the notification of changes in the privacy policy to users and the audit of accesses to users' PHRs, as shown in Table 2.

Table 2. Characteristics of each PHR system. PL: Privacy policy location; DS: Data source; DM Data managed; AM: Access management; AA; Access audit; DA: Data accessed without the user's permission; SM: Security measures; CP: Changes in privacy policy; S: Standards.

Tool	PL	DS	DM	AM	AA	DA	SM	CP	S
1. Google Health	1	4	1	1	1	3	3	2	1
2. ZebraHealth	2	1	0	0	0	1	3	4	1
3. myHealthFolders	1	1	2	2	1	1	3	1	0
4. Keas	1	4	1	0	0	2	3	3	0
5. EMRy Stick Personal Health Record	2	1	1	0	1	1	0	0	0
6. My HealthVet	2	1	1	2	0	1	2	0	1
7. myMediConnect	0	3	1	2	0	0	3	0	1
8. MyChart	1	2	1	0	1	4	0	0	1
9. MedicAlert	1	1	1	3	0	2	3	2	0
10. Microsoft HealthVault	1	4	1	4	1	1	3	2	3
11. MediCompass	1	5	1	2	0	2	3	0	3
12. TeleMedical	1	1	2	0	0	0	2	2	2
13. Health Butler	1	1	1	2	0	2	0	4	0
14. NoMoreClipBoard.com	1	3	2	2	1	2	2	2	1
15. MiVIA	1	0	1	2	0	3	3	2	1
16. iHealthRecord	1	0	0	0	0	1	2	4	0
17. Dr. I-Net	1	3	1	2	0	0	3	0	0
18. My Doclopedia PHR	1	2	1	2	0	3	2	2	1
19. dLife	1	0	0	0	0	4	2	2	0
20. RememberItNow!	1	4	1	4	1	3	2	3	0
21. MedsFile	1	1	1	0	1	4	1	1	0
22.Juniper Health	1	1	2	0	0	2	3	2	0

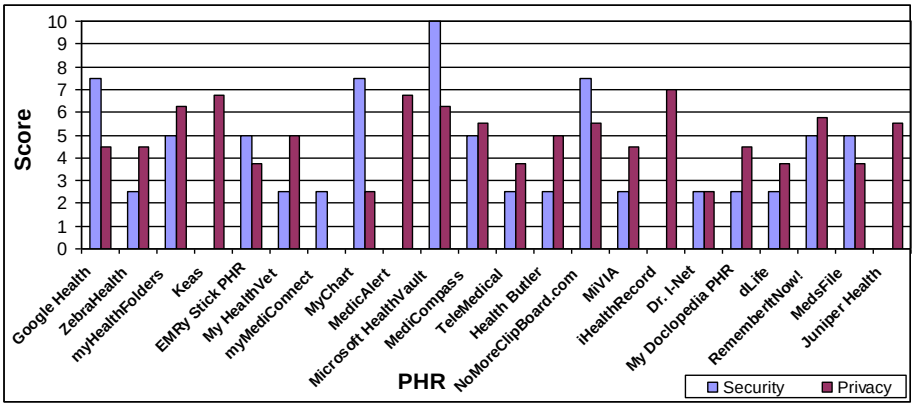

Fig. 1. PHRs usability score distribution.

5 Conclusions

In this paper, a survey of 22 free web-based PHRs has been carried out. Most PHRs (86.36%) access different kinds of information without the users' explicit consent, but access to their identified information without their consent is never acceptable. Only thirteen PHRs (59.09%) notify or announce changes in their privacy policy to users. A number of PHRs (40.90%) do not provide any information about how the users provide access to their PHR data. In three PHRs (13.64%), physical security measures and electronic security measures are not reported. The Privacy Policies must include this aspect in order for users to perceive that their information will be protected by the PHR system. In a large number of PHRs (63.64%) the users cannot see an audit of accesses to their PHRs. This aspect should be improved because the users should be aware of how their information has been shared. A number of the PHRs reviewed (36.36%) are not regulated by a standard setting body. In future work, we intend to extend our analysis to a wider sample of PHRs, and compare the security and privacy features of free web-based PHRs with proprietary web-based PHRs.

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

References

1. Sood, S.P., Nwabueze, S.N., Mbarika, V.W.A., Prakash, N., Chatterjee, S., Ray, P., Mishra, S.: Electronic Medical Records: A Review Comparing the Challenges in Developed and Developing Countries. HICSS '08, IEEE Computer Society, Washington, DC, USA (2008),
2. Connecting for health personal health working group. connecting for health. the personal health working group final report (2003),

http://www.providersedge.com/ehdocs/ehr_articles/The_Personal_Health_Working_Group_Final_Report.pdf.
3. myMediConnect Personal Health Records, http://www.mymediconnect.net/phr.php
4. Tang, P.C., Ash, J. S., Bates, D.W., Overhage, J.M., Sands, D.Z.: Personal health records: Definitions, benefits, and strategies for overcoming barriers to adoption. J Am Med Inform Assoc 13(2), 121-126 (2006)
5. Farzandipour, M., Sadoughi, F., Ahmadi, M., Karimi, I.: Security requirements and solutions in electronic health records: Lessons learned from a comparative study. Journal of Medical Systems 34(4), 629-42 (2010)
6. ISO/TS 13606-4. Health informatics Electronic health record communication part 4: Security (2010), http://www.iso.org/
7. Birge, C.: Enhancing research into usable privacy and security. In: Proc. of the 27th ACM international conference on Design of communication, pp. 221-226. SIGDOC '09, ACM, New York, USA (2009)
8. Martino, L., Ahuja, S.: Privacy policies of personal health records: an evaluation of their effectiveness in protecting patient information. In: Proc. of the 1st ACM International Health Informatics Symposium, pp. 191-200. IHI '10, ACM, New York, USA (2010)
9. Review of the Personal Health Record (PHR) service provider market: Privacy and security. ALTARUM Research (January 2007), http://www.hhs.gov/healthit/ahic/materials/01_07/ce/PrivacyReview.pdf
10. Detailed PHR privacy report cards. Patient Privacy Rights Foundation (2010), http://patientprivacyrights.org/detailed-phr-privacy-report-cards
11. User Centric (2010), http://www.usercentric.com/publications/2009/02/02/googlehealth-vs-microsoft-healthvault-consumers-compare-onlinepersonal-hea
12. Kotz, D., Avancha, S., Baxi, A.: A privacy framework for mobile health and home-care systems. In: Proc. of the first ACM workshop on Security and privacy in medical and home-care systems, pp. 1-12. SPIMACS '09, ACM, New York, USA (2009)
13. Mohan, A., Blough, D.M.: An attribute-based authorization policy framework with dynamic conflict resolution. In: Proc. of IDTRUST '10, pp. 37-50, ACM, New York, USA (2010)
14. Williams, J.: Social networking applications in health care: threats to the privacy and security of health information. In: Proc. of the 2010 ICSE Workshop on Software Engineering in Health Care, pp. 39-49. SEHC '10, ACM, New York, USA (2010)
15. Huang, L.C., Chu, H.C., Lien, C.Y., Hsiao, C.H., Kao, T.: Privacy preservation and information security protection for patients' portable electronic health records. Comput. Biol. Med. 39, 743-750 (September 2009)
16 I. Carrión, J.L. Fernández Alemán, and A. Toval, “Assessing HIPAA standard in practice: PHRs Privacy Policies”, In: Proc. of IEEE EMBC’11, (2011) (accepted for publication)
17. Sunyaev, A., Chornyi, D., Mauro, C., Krcmar, H.: Evaluation framework for personal health records: Microsoft healthvault vs. google health. In: Proc. of the 2010 43rd Hawaii International Conference on System Sciences, pp. 1-10. HICSS'10, IEEE, (2010)
18. Sunyaev, A., Kaletsch, A., Krcmar, H.: Comparative evaluation of Google Health API vs. Microsoft Healthvault API. In: Proc. of the Third International Conference on Health Informatics, pp. 195-201. (2010)
19. Cushman, R., Froomkin, A.M., Cava, A., Abril, P., Goodman, K.W.: Ethical, legal and social issues for personal health records and applications. J. of Biomedical Informatics 43, S51-S55 (October 2010)
20. Hulse, N.C., Wood, G.M., Haug, P.J., Williams, M.S.: Deriving consumer-facing disease concepts for family health histories using multi-source sampling. Journal of Biomedical Informatics 43(5), 716-724 (October 2010)
21. HIPAA (2010), http://www.cms.gov/HIPAAGenInfo
22. Boyer, C., Selby, M., Scherrer, J.R., Appel, R.D.: The health on the net code of conduct for medical and health websites. Computers in Biology and Medicine 28(5), 603-610 (1998)